LEGAL IMPLICATIONS OF THE USE OF BIOMETRICS AS A TOOL TO FIGHT THE GLOBAL WAR ON TERRORISM

A thesis presented to the Faculty of the U.S. Army Command and General Staff College in partial fulfillment of the requirements for the degree

MASTER OF MILITARY ART AND SCIENCE
Homeland Security

by

CATHERINE M. BLACK, MAJOR, USA
B.S., Campbell University, Buies Creek, NC, 1997

Fort Leavenworth, Kansas
2008

.
Approved for public release; distribution is unlimited.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
13-06-2008	Master's Thesis	AUG 2007 – JUN 2008

4. TITLE AND SUBTITLE

Legal Implications of the Use of Biometrics as a Tool to Fight the Global War on Terrorism

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

BLACK, CATHERINE M., MAJOR, USA

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
U.S. Army Command and General Staff College
ATTN: ATZL-SWD-GD
Fort Leavenworth, KS 66027-2301

8. PERFORMING ORG REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for Public Release; Distribution is Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Since the fall of the Soviet Union and the emergence of the United States (US) as the single world superpower, the focus of the Army has shifted its threat paradigm from a focus on the Communist threat to that of multiple threats from both nation states and non-state actors. The terrorist attacks against the United States Homeland on September 11, 2001 highlighted the need for the country's leadership to develop effective means of identifying personnel as a part of a national security plan. National security agents identified many of the perpetrators of the 9/11 attacks as posing a threat to the US; however, their failure to apprehend the suspects led to the terrorist attacks. If the country employed biometric technologies in the airports prior to the attacks, it is likely that the Federal Bureau of Investigation (FBI) would have identified and detained the suspects, thwarting their plan to terrorize innocent citizens.

A biometric identification system would certainly present law enforcement officials with a powerful tool for the identification of known or suspected terrorists and other criminals, however, the system must adhere to the laws designed to protect the individual privacy of US citizens while providing an effective means of identifying known and suspected criminals. To develop such a program, system designers would have to ensure that the program adheres to the Fourth, Fifth, and Fourteen Amendments of the US Constitution while providing consideration for the Privacy Act and the Patriot Act.

15. SUBJECT TERMS
Biometrics

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. PHONE NUMBER** *(include area code)*
(U)	(U)	(U)	(U)	86	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18

MASTER OF MILITARY ART AND SCIENCE
THESIS APPROVAL PAGE

Name of Candidate: Major Catherine M. Black

Thesis Title: Legal Implications of the Use of Biometrics as a Tool to Fight the Global War on Terrorism

Approved by:

_____, Thesis Committee Chair
O. Shawn Cupp, M.M.A.S.

_____, Member
BG William D. R. Waff, D.Min.

_____, Member
LTC Misti Stowell, J.D.

Accepted this 13th day of June 2008 by:

_____, Director, Graduate Degree Programs
Robert F. Baumann, Ph.D.

The opinions and conclusions expressed herein are those of the student author and do not necessarily represent the views of the U.S. Army Command and General Staff College or any other governmental agency. (References to this study should include the foregoing statement.)

ABSTRACT

LEGAL IMPLICATIONS OF THE USE OF BIOMETRICS AS A TOOL TO FIGHT THE GLOBAL WAR ON TERRORISM, by Major Catherine M. Black USA, 86 pages.

Since the fall of the Soviet Union and the emergence of the United States (US) as the single world superpower, the focus of the Army has shifted its threat paradigm from a focus on the Communist threat to that of multiple threats from both nation states and non-state actors. The terrorist attacks against the United States Homeland on September 11, 2001 highlighted the need for the country's leadership to develop effective means of identifying personnel as a part of a national security plan. National security agents identified many of the perpetrators of the 9/11 attacks as posing a threat to the US; however, their failure to apprehend the suspects led to the terrorist attacks. If the country employed biometric technologies in the airports prior to the attacks, it is likely that the Federal Bureau of Investigation (FBI) would have identified and detained the suspects, thwarting their plan to terrorize innocent citizens.

A biometric identification system would certainly present law enforcement officials with a powerful tool for the identification of known or suspected terrorists and other criminals, however, the system must adhere to the laws designed to protect the individual privacy of US citizens while providing an effective means of identifying known and suspected criminals. To develop such a program, system designers would have to ensure that the program adheres to the Fourth, Fifth, and Fourteen Amendments of the US Constitution while providing consideration for the Privacy Act and the Patriot Act.

ACKNOWLEDGMENTS

I would first like to thank my son Alexander for his patience and his support. He served as a constant cheerleader, and often put on an interested expression and pretended to care when I shared numerous mundane facts with him. I would also like to thank my Mother, my brothers, my sister-in-law, my niece, and my nephews for their support. It is for my son, my niece, my nephews and their children that I write this paper in hopes that one day some of the thoughts and ideas proposed in this work will help create a more secure country for them and their children. It is my hope that they will be able to live the American dream without undue fear of terrorist activities of other nation states and super-empowered angry people, and that they will enjoy all of the freedoms and rights that are due to them as US citizens. I wish them all of the happiness and blessings that this world has to offer. I challenge them to live with the knowledge that freedom is never free; that its price is the blood and sacrifices of those who came before them, and that it is up to them to continue to secure that freedom for future generations. I would also like to thank my best friend Mary who constantly reminded me that I could "MASTER" anything, including an MMAS.

Finally, I would like to express my heartfelt thanks to my committee: Mr. Cupp, BG Waff, and LTC Stowell for their patience, wisdom, expertise, and guidance. I felt very privileged to work with a group of talented and wise professionals who went well beyond the call of duty to assist me in the development of a product worthy of an MMAS. My deepest and most sincere thanks go out to all of you.

TABLE OF CONTENTS

Page

ACRONYMS

ACLU	American Civil Liberties Union
BAT	Biometric Automated Tool Kit
BSC	Biometric Support Center
COA	Course of Action
COF	Commercial Off-the-Shelf
DHS	Department of Homeland Security
EPIC	Electronic Privacy Information Center
FBI	Federal Bureau of Investigation
FTC	Federal Trade Commission
GWOT	Global War on Terrorism
HIIDE	Hand-Held Interagency Identity Detection Device
IAFIS	Integrated Automated Fingerprint Identification System
IDENT	Automated Biometric Identification System
INS	Immigration and Naturalization Service
NIST	National Institute of Standards and Technology
SSA	Social Security Administration
SSB	Social Security Board
SSN	Social Security Number
UAE	United Arab Emirates
US	United States
US-VISIT	United States Visitor and Immigrant Status Indicator Technology
USCG	United States Coast Guard

CHAPTER 1

DEFINING THE PROBLEM

Introduction

Governments and law enforcement agencies used biometrics for quite some time to identify personnel; however, computer technologies increased the utility of biometrics over time. Standard fingerprinting techniques date back to 1901 when the detectives of Scotland Yard began to use them in criminal investigations (Encyclopedia Britannica online, s.v. "Fingerprinting," http://www.britannica.com/ebc/article-9364450 (accessed October 2, 2007)). Since then, the repertoire of biometric tools has increased dramatically. Today there are a number of biometric tools available for use by the federal government and law enforcement agencies to include signatures, fingerprints, retinal scans, iris scans, DNA, hand geometry, voice recognition, facial recognition, and other emerging technologies. Several United States (US) government agencies currently exploit these technologies to protect the citizens of the US from terrorist threats (Kaucher 2007). In 2004, US military organizations used over 100 digital fingerprint and iris scanners in Iraq to assist in the control of access to military facilities, to gather information on known dissidents, and to assist in the hiring and administrative control of Iraqi contract workers (Onley 2004).

To discuss all of the biometric tools available is beyond the scope of this paper. Though research concerning many different biometric tools is presented, the major focus is on the biometric tools available as part of the Biometric Automated Tool Kit (BAT) (Onley 2004), a portable system, developed in the Army's Battle Command Laboratory in Fort Huachuca, Arizona, that includes a retinal scanner, digital camera, and digital

fingerprint collector. This system allows for the capture, storage, comparison, and retrieval of biometric information, and assists US government agencies in the identification, capture, and detention of known or suspected terrorists (Kenny 2005).

Primary and Secondary Research Questions

Though there is a significant amount of research available concerning the application of biometric technologies, the amount of research concerning the legal implications associated with biometrics is quite limited because the technologies develop at a much faster rate than the laws that govern their use. With the assistance of computer technologies, biometrics will certainly outpace the development of laws to regulate their use for years to come. This gap between technological development and the implementation of laws to regulate the use of the technologies will likely cause great concern for a significant number of American citizens as the functionalities of biometrics begin to infiltrate everyday life, robbing individuals of the deeply held American value of privacy.

Freedom is a deeply held American value. The names of Operations Enduring Freedom and Iraqi Freedom point to a deep American desire not only to secure its own freedom, but also to project that freedom throughout the world. US government agencies may freely collect biometric information from citizens of Afghanistan and Iraq (Biometrics Task Force 2007), and store it in databases without significant legal concern; however, privacy laws and the constitution limit the government's ability to collect and store biometrics of US citizens. In addition to legal regulation, several organizations such as the American Civil Liberties Union (ACLU) and the Electronic Privacy

Information Center (EPIC) service as watchdogs to protect American civil liberties and privacy (Electronic Privacy Information Center 2007).

Many Americans see the use of biometrics as a means of limiting their freedoms and right to privacy. The need for American security following the terrorist attacks on 9/11, challenges the American desire for freedom. Most would agree to forego some of their freedoms to increase the security of the nation; however, they would be rightfully concerned that the government takes the appropriate steps to protect individual rights and freedoms while protecting them from terrorist threats. Since biometrics present government and security officials an unprecedented ability to identify many suspected or potential terrorists and other criminals, it would be negligent to fail to integrate biometrics into security plan designed to protect the homeland. Given that the use of biometrics is expanding at an unfettered rate, the US government must consider strategies that provide both security from the threat, as well as preserve individual privacy. This causes one to ask how the US government may use biometrics as a legitimate component of a comprehensive security initiative. Which biometric markers should security officials use to collect information, and by what means should government officials collect the information? Finally, how should security officials store and protect information from misuse and compromise?

Significance of the Research

Many would agree that biometric technologies are here to stay. They do not represent a fad that will go away with time, but a valuable tool for use in many situations, from the identification of criminals, to the identification of high school students to ensure

that cafeteria workers charge the appropriate accounts for daily lunches. Effective management strategies may increase their efficiency and reduce the probability of abuse.

As stated previously, freedom and privacy are American values. The Fourth, Fifth, and Fourteenth amendments of the US Constitution protect individual citizens' rights and freedoms. The US Congress passed the Privacy Act of 1974 to clarify the legal right to individual privacy; however, following the terrorist attacks on 9/11, Congress passed the Patriot Act, which placed a number of limitations on personal privacy, with the intent of thwarting terrorist plots against the US and its interests. When one considers the value that biometrics may add to the security of the US, one must consider it alongside the various laws enacted to protect the freedoms that US citizens enjoy.

Limitations

Due to the complexity of this topic, it is beyond the scope of this research to discuss every available biometric technology. The research will therefore focus on the biometric technologies associated with the Army Battle Command Laboratory's Biometrics Automated Tool Kit (Onley 2004). The BAT allows security personnel to record iris scans, fingerprints, and digital photographs using a portable iris scanner, digital fingerprint collector, and digital camera (Deconta and Iasso 2006). Discussion is also limited to the legal considerations, and the laws associated with the use of biometric technologies and its associated databases within the US. There remains a strong need for research into the ethical considerations associated with using biometrics as a means of identifying American civilians.

The classified community uses a number of biometric technologies to further their prosecution of the Global War on Terrorism (GWOT); however the use of classified technologies is beyond the scope of this paper. Further research into the use of biometrics within the classified community may be valuable as it may have great utility in identifying and capturing terrorists.

Assumptions

The author assumes that most Americans value their individual privacy, and are opposed to the government's unfettered use of biometrics, and that many Americans and civil organizations would oppose the use of biometric databases to store personal information because of the potential threats to personal freedoms, and invasion of privacy. The author also assumes that the implementation of recommended strategies are cost-effective to the US government and law enforcement agencies, and that they would be valuable in prosecuting the GWOT.

Though it is an emerging technology, a wealth of information concerning biometrics is available. This document addresses a number of constitutional amendments and legal opinions associated with the use of biometric technologies in the US. Chapter 2 discusses the extensive amount of information concerning biometrics and its legal implications. It discusses many of the different biometric technologies available for use by the US government and other organizations as part of the GWOT, as well as literature concerning the legal implications of biometric collection and storage within databases in the US. Chapter 3 discusses Constitutional Amendments and laws associated with the use and storage of biometric information collected against US citizens, and presents

possible COAs that the federal government may choose when developing a biometric security program.

Chapter 4 analyzes the COAs presented in chapter 3, and discusses many of the advantages and limitations associated with using various COAs while presenting case studies as a means to further explore the COAs. It presents a viable protocol for collecting biometrics, and recommends a COA that best capitalizes on the technology while taking into consideration the legal rights of US citizens.

Chapter 5 justifies the COA that the researcher selects in chapter 4. It provides justification to support the COA, and examine the merit of implementing the COA as part of a security program designed to assist in the prosecution of the GWOT. It discusses possible future uses of biometrics by the US government, and ends by suggesting further research that lies outside of the scope of the document.

CHAPTER 2

LITERATURE REVIEW

Introduction to Biometrics

The US government uses many different biometric technologies to identify personnel. Prior to entering a lengthy discourse on the government's use of biometrics, it is appropriate to first describe and discuss some of the biometric tools available to the US government. Since it is probably the most widely used biometric, familiarization with biometric techniques will begin with the fingerprint.

Fingerprinting

As stated in chapter 1, Scotland Yard introduced fingerprinting as a viable biometric tool in 1901 (Encyclopedia Britannica online, s.v. "Fingerprinting," http://www.britannica.com/ebc/article-9364450 (accessed October 2, 2007)). Fingerprinting techniques advanced significantly since the days of their introduction to Scotland Yard. At the beginning of the fingerprinting era, law enforcement personnel collected fingerprints by requiring suspected criminals to place their fingertips in ink to make impressions on paper (Holcomb 1959). Technicians compared fingerprint impressions of the suspected criminals to latent fingerprints found at crime scenes to link the suspect to the crime. Officers revealed latent fingerprints by applying a fingerprinting dust to various surfaces at the crime scene using a soft brush. The dust would adhere to moisture and other deposits left by the ridges on the fingerprint, revealing the latent print. The technology was not ideal. The mechanical nature of dusting for latent fingerprints often significantly degraded the latent print. Additionally, the quality of the fingerprint

varied with the skill of the fingerprinting technician, the dyes, and the inks used to make the impression and the depth of the ridges on the print (Gaensslen and Lee 2001). Though similar technologies are still employed to this day, current technology allows for the digital scanning of both fingerprints and latent fingerprints. Once scanned, technicians enter digital representations of fingerprints and latent fingerprints into databases for future comparison or retrieval.

There are two basic fingerprinting techniques: rolled and flat fingerprinting. Fingerprint technicians use both techniques in inkblot and digital scanning (Rosenzweig et al., 2004). In digital scanning, technicians collect flat fingerprints by exposing the pad of the fingertip to a digital scanner, which collects a digital image of the fingerprint. In the case of inkblot collection, the technician exposes the pad of the finger to ink, and then makes an impression of the fingerprint on paper. This method allows for the collection of only the pad of the fingertip. Technicians collect rolled digital fingerprints by placing the side of the finger on a scanner, and rolling the finger from one side to the other, exposing the front and sides of the finger to the scanner. In the case of ink blot collection, the technician exposes the front and sides of the finger to ink, then makes an impression of the fingerprint by rolling the finger from on side to the other, on paper, allowing for the capture of the front and side sections of the finger.

Rolled fingerprinting is the preferred technique because it provides more biometric information than does flat fingerprinting, leading to greater accuracy when comparing fingerprints. Digital scanning is preferred over inkblot printing because digital collection allows for the immediate encryption and electronic storage of the fingerprint. Conversion of inkblot prints to digital templates is possible; however, some

distortion of the print may occur during conversion. In any case, digital storage is preferred over the storage of a paper print because paper prints require a significant amount of storage space, and the paper and or the print may degrade over time. In addition to requiring less storage space, digital storage in databases allows for the computerized comparison of fingerprints, which greatly increases throughput capacity when compared to comparing samples using the naked eye (Adkins 2007).

Fingerprints are quite useful biometrics when they are accessible; however, they may not be available. In many cases, the perpetrator of a crime uses gloves to ensure that he leaves no fingerprints. In other cases, the perpetrator of the crime may alter his fingerprints in an effort to evade prosecution. According to Dr. Thomas Amerson of the US Coast Guard (USCG) Research and Development Center, many felons and other criminals alter their fingerprints by various means. Their techniques include using acids or sandpaper to remove the telltale ridges on their fingertips used in fingerprinting. He also notes that some individuals graft skin from other parts of their bodies and attach the grafted skin to their fingers using stitching or glue in an effort to conceal their true fingerprints (Amerson 2007). In cases such as these, fingerprints alone may not be sufficient to provide positive identification, requiring the employment of other biometric identifiers.

The USCG benefited significantly from the use of biometrics as a part of their effort to defend the US maritime borders (Pentagon Channel Recon 2008). The USCG constantly patrols the Mona Pass between the Dominican Republic and Puerto Rico to prevent illegal immigrants from infiltrating the US. Prior to the use of biometrics by the

USCG, cutter crews interdicted over ten thousand people each year as they attempted to immigrate illegally to the US through the Mona Pass (Amerson 2007).

The Mona Pass is a primary route for illegal immigrants traveling from the Dominican Republic to the US. The Pass is a 90-mile waterway between the Dominican Republic and Puerto Rico. It is a navigable passageway preferred by many illegal immigrants who wish to infiltrate to the US by boat. This route is particularly suited for the Dominicans because they speak Spanish, and are able to infiltrate Puerto Rican society with ease. The Dominicans build small wooden boats known as yolas to ferry the illegal immigrants through the pass. The boats are hand-made vessels powered by sails and sometimes outboard motors crowded with as many people as possible with no safety equipment, water, or food. Though the USCG has no statistics to confirm the number of immigrants that travel this route, it is highly likely that many of the yolas sink, drowning the riders. In many cases, USCG cutters locate capsized yolas and rescue the travelers (Amerson 2007).

Prior to the use of biometrics by the cutter crews in the Mona Pass, the crews would locate overcrowded or capsized yolas, and proceed to rescue the illegal immigrants. They would provide life vests to all of the illegal immigrants, move them onto the cutter, and destroy the yola. After providing them with food, water, and emergency medical treatment, the crew would return them to the Dominican Republic. Since the USCG had no means of identifying the personnel, there were essentially no legal consequences for having attempted to illegally migrate to the US, so many of those who were returned to the Dominican Republic would make multiple attempts to enter the US via the Mona Pass. The cutter crews captured some illegal immigrants so frequently

that the illegal immigrants knew some of the members of the cutter crews by name. The cutter crews would also routinely encounter illegal immigrants, whom they previously captured and returned to the Dominican Republic, living in Puerto Rico after successful illegal migration to the US (Pentagon Channel Recon 2008).

The cutter crews would become exhausted with the task of ferrying illegal immigrants back to the Dominican Republic. Transporting the migrants was quite complicated as a typical cutter only carries a crew of sixteen, while the overcrowded yolas routinely carry over 100 passengers, capable of taking over the cutter with relative ease. The crews have to keep the illegal immigrants on the deck of the cutter exposed to the elements during the ride back to the Dominican Republic to prevent the illegal immigrants from taking over the vessel. The crew maintains a stock of life vests, food, water, and medical supplies for illegal immigrants whom they expect to encounter in the Pass. The passengers must use a toilet on the deck of the cutter that provides them with no privacy during the trip. Worst of all, the cutter crews would risk their lives to rescue the immigrants knowing that they would make multiple attempts to illegally cross the Pass (Pentagon Channel Recon 2008).

In 2005, the USCG began using biometrics to identify the illegal immigrants they apprehended in the Mona Pass. The introduction of biometric systems to the USCG in this instance caused revolutionary change in the processing and prosecution of illegal immigrants crossing the Pass. The cutter crews began to carry with them portable fingerprint/digital photo collection devices to collect biometric data from the migrants. The collection devices allow the crew to email digital images of the migrants' fingerprints and digital photos of the migrants via satellite to United States Visitor and

Immigrant Status Indicator Technology (US-VISIT). The US-VISIT program is a border control initiative that requires persons entering the US to provide digital photos and fingerprints to the border patrol. The collection of biometrics by the border patrol serves to assist agents in the identification of persons entering and exiting the US. Biometric collection and enrollment of individual data allows the Department of Homeland Security (DHS) to verify the identity of personnel entering and exiting the US, as well as to identify known or suspected criminals as they attempt to enter or exit the US (Amerson 2007). The US-VISIT database currently holds over 100 million records of individuals entering or exiting the US.

The US-VISIT database interacts with the FBI's Integrated Automated Fingerprint Identification System (IAFIS), which carries a database containing digital images of fingerprints of known or suspected criminals (Federal Bureau of Investigation 2007). The system infrastructure allows for the comparison of the immigrants' fingerprints to those in the US-VISIT and IAFIS databases to determine whether or not the immigrant in question has previously attempted to illegally immigrate to the US, if he appears on a terrorist watch list, or if he has outstanding warrants for arrest in the US. This system works without human interaction. When the system generates a number of possible matches to an immigrant's fingerprints, the system sends the fingerprint along with all of the potential matches to a Biometric Support Center (BSC), where professional fingerprint analysts work 24-hours a day comparing fingerprints. Within ten minutes or less, the BSC staff determines whether the migrant's fingerprints match one of the "best match" fingerprints selected by the computerized system (Amerson 2007).

The computerized system also sends questionable fingerprints to the BSC. This allows the fingerprint analysts to "see" the fingerprints to determine whether they have been altered. This functionality is necessary because many criminals attempt to remove or alter their fingerprints in order to defeat the efforts of law enforcement officials. Illegal immigrants and other criminals may attempt to remove their fingerprints using sandpaper or acid. In some cases, criminals had their fingerprints surgically altered by grafting skin from their toes or other body parts to their fingertips. Current technology assists in the detection of altered fingerprints. Some technologies trace the flow of blood in capillaries that follow that natural grooves and ridges of the fingerprint to determine whether they match the actual fingerprint. Through the detection of the capillary flow, this technology also determines if the captured fingerprint is from a live person. This prevents the use of rubberized or other prosthetic devices designed to defeat the system. In addition, since the capillary flow follows that of the natural fingerprint, current technology can produce a digital representation of the true fingerprint even when the criminal has removed or altered the fingerprint (Amerson 2007).

During computer analysis, technicians compare collected fingerprints and digital photos to those in existing terrorist and other criminal databases to determine whether the individual has a criminal history. The technicians enroll fingerprints and digital photos that do not exist in the database in the system along with biographic information to record the immigrant's attempt to infiltrate the US. US-VISIT records biometric information on all members of the immigrant party attempting to cross the Pass, and annotates the time and location of the apprehension of the illegal immigrants. If the individual has no outstanding warrants, and has no previous record for attempted illegal entry, the cutter

crew returns him to the Dominican Republic. If the individual has outstanding warrants or has a previous citation for attempting to enter the US illegally, the cutter takes the individual to Puerto Rico where local law enforcement officials take the individual into custody, and begins the process to prosecute him. Note that the computerized analysis only compares fingerprints of the personnel. The current USCG model has no facial recognition capability. The digital photo exists to confirm the identity of the individual in the event that computerized analysis produces more than one possible fingerprint match (Amerson 2007).

The system serves as both a powerful tool for deterrence and prosecution of those who attempt to enter the US illegally. Prior to the introduction of biometrics, the government rarely prosecuted illegal immigrants because it was difficult to establish their identity. The illegal immigrants were only subject to prosecution if they performed heinous acts during their capture such as failing to heave-to, assaulting crewmembers, or firing upon the cutter. In 2006, though the cutters captured over ten thousand illegal immigrants, the courts only prosecuted one. During the first half of the year 2007, following the introduction of biometric systems, the courts prosecuted sixty-eight illegal immigrants. The current positive "hit rate" for fingerprints collected from migrants within the Mona Pass is approximately 20 percent. This includes those who have previously attempted to enter the US illegally as well as other known and suspected criminals. Since the implementation of the program, the USCG witnessed a reduction in illegal migrant traffic along the Mona pass of approximately 50 percent. The USCG attributes this reduction to the deterrent effect of the biometric identification program, the arrest of repeat offenders, and an aggressive media campaign within the Dominican

Republic designed to discourage potential illegal immigrants from traveling by yola through the Mona Pass. Currently the USCG only uses the biometric security plan in the Mona Pass, however, due to the effectiveness of the program; the USCG is expanding the program to include other well-traveled routes (Amerson 2007).

Facial Recognition

A second biometric, facial recognition, is based on the principle that people seem to possess the innate ability to distinguish between facial characteristics. Facial recognition technology attempts to mimic the human ability to distinguish between people based on facial characteristics (Rosenweig et al., 2004). It compares images of live persons or static photos to stored templates (Rosenzweig et al., 2004). Digital photos, like those taken of Mohammad Atta, one of the hijackers of the 1991 terrorist attacks against the Pentagon and the World Trade Center, allowed for his identification during the investigation following the attacks (MacVicar 2001).

Some facial recognition technologies allow security personnel to watch live video feed of people as cameras passively collect their images. This technology is very useful in monitoring areas that should be vacant. A security agent monitoring a department store through closed circuit television, for example, can alert security guards to investigate if he sees video of a person walking through the store after hours. This use of the technology only informs the user that a person is in a restricted area. It does not reveal the intruder's identity. More advanced technologies provide high-resolution images that allow security personnel to compare the facial features of the suspected intruder to pictures of known or suspected criminals (Feder 2003).

Security agents used advanced facial recognition technologies during the February 2002 Super Bowl. Following the September 2001 terrorist attacks, law enforcement personnel expressed great concern for the security of US citizens attending public events. The Super Bowl, attended by over 100,000, and televised internationally, presented potential terrorists with an opportunity to execute a spectacular attack against unsuspecting civilians. Law enforcement agencies responded by employing facial recognition technologies. The technology converted spectators' facial images into digital templates and compared the spectators' facial characteristics to those of known or suspected terrorists and other criminals. During the football game, law enforcement officials scanned the crowd of over 100,000 spectators to identify known felons and persons associated with terrorist groups in an effort to avert a potential terrorist attack. (Rutherford 2001).

According to police and FBI records, law enforcement personnel made no arrests based on the use of the facial recognition programs, though the system identified 19 facial matches. It is unclear; however, how many of these matches were "true matches." A match is confirmed when a law enforcement official approaches the individual and confirms his identity. One should not conclude that because police made no arrests that none of the 19 facial matches were true matches. An officer, for example could have positively identified a scalper with the use of the technology, but did not to arrest him to conserve resources for use in the event that a terrorist or other dangerous criminal found his way into the area (Woodward et al., 2002).

Heathrow Airport, in London, England, employs advanced facial recognition technologies as a part of a comprehensive security plan. Security personnel monitor

digital images of travelers as they pass through the airport. Studies conducted by volunteers in 2007 revealed an 85 percent accuracy rate in correctly identifying persons based on facial characteristics, even when the volunteers attempted to conceal their facial features using additional facial hair and sunglasses. Heathrow Airport security management personnel hope to employ technologies that not only passively collect travelers' digital facial images, but also passively collect iris scans (Friedlos 2007).

The Carnegie Mellon CyLab in Pennsylvania, one of the country's leading biometrics labs, is committed to the development of increasingly accurate biometric technologies. One of their current programs seeks to improve the accuracy of facial recognition technologies. Illumination, expression, and orientation greatly affect the accuracy of these technologies. One need only to watch the daily news to see distorted images of criminals caught in the act of robbing convenience stores. The store cameras often collect distorted images of the suspect, limiting their value to law enforcement. The CyLab seeks to develop technologies that adjust lighting and resolution of digital images to make them more useful to law enforcement officers. They are also developing technologies designed to normalize facial features. This technology allows for the identification of facial features even when the individual employs multiple expressions. It is important because many people can become very difficult to identify when they change expressions. They are also developing technologies that can identify exaggerated facial expressions because criminals often employ different facial expressions with the intent to defeat facial recognition technologies or to prevent witnesses from recognizing them based on their facial features (Bhagavatula 2007).

Iris Scanning

Though a facial match rate of 85 percent seems impressive, it is clear that facial recognition technologies require more research and development to become a more effective tool for law enforcement. Iris scanning and retinal scanning produce much more accurate results. Iris and retinal scanning are similar technologies. As early as the 1930s, research suggested that the pattern of blood vessels in the retina was unique to individuals; however, it took and additional fifty years for the company "EyeDentify" to develop the technology required to capture retinal scans (National Center for State Courts 2007).

Retinal scanners collect biometric information by scanning the optic nerve, located at the back of the eye (Woodard et al., 2003). After collection, technicians enter the data into databases in digital form for later use. As early as the 1930s, scientists proposed that the iris of each person is unique. Interestingly, John Daugman, a professor at Harvard University, developed the algorithms necessary to develop the technology in 1994 following the fictional use of the technology in a James Bond film (National Center for State Courts 2008). Researchers identified approximately 266 characteristics of the iris that may be used as unique biometrics. A typical iris scanner captures approximately 173 of these characteristics (Rosenweig et al., 2004). Both iris and retinal scanners require the subject to focus on a point while a scanner collects a digital image of the iris or retina. Like the other technologies, technicians record the resulting template in a database for future use.

The United Arab Emirates (UAE) uses biometrics to control entry into and exit from the country. As the "Las Vegas" of the Middle East, people visit the UAE in droves

each year seeking business opportunities and entertainment. The country expelled or banned a significant number of people from the country for committing various crimes during their visits. In order to ensure that these people do not return to the country, border agents collect biometric data in the form of retinal scans from every individual as he or she enters the country. The agents use computer technologies to compare the travelers' iris scans to iris scans of people on the country's list of expelled personnel. If the individual's iris scan matches one of the iris scans of a person on the watch list, border patrol agents deny the traveler entry (Rosenweig et al., 2004).

Prior to the use of retinal scans as a tool to monitor its borders, agents would compare names on passports to names on the country's watch list. This method was time-consuming, and quite ineffective. Many people, after expulsion from the UAE, would return to their home countries, change their names and other personal data, obtain new passports and reenter the UAE undetected. Retinal scanning brought to the UAE border patrol a much more effective and efficient identification system. Instead of relying on the border patrol agent's ability to recognize fraudulent passports, and to recognize expelled personnel based on individual facial recognition, they now rely on the iris scans to identify personnel. As of 2004, the biometric database used to control entry into the UAE contained over 632,500 iris scans, enrolling over 600 new irises each day, and denying entry to approximately 30 people per day, with an estimated false positive error estimate of 1 in 80 billion (Rosenweig et al., 2004).

Public Objection to the Use of Biometrics

Given its effectiveness, one might wonder why such technologies are not used to the same extent in the US. The US has actively sought to control its borders since the

terrorist attacks on September 11, 2001. Why would the US not adopt a proven system to use in the effort to identify and capture terrorists? The answer is not a simple one. According to John Woodard and others, of the RAND Corporation, there are a number of socio-cultural concerns associated with the use of biometrics in the US. The concerns enumerated by this think tank are physical privacy, informational privacy, and religious objections (Woodard et al., 2001).

Physical Privacy

Physical privacy concerns, as described by RAND, fall into three categories: physical harm, stigmatization, and hygiene (Woodard et al., 2001). Woodard's group has found no evidence that biometric collection causes physical harm, however, their research does not address the perception that some have that the use of biometrics can cause physical injury to either the person collecting the biometric sample or the subject from whom the sample is taken. One may be concerned that a retinal scan, for example, may cause damage to the eye, or that the scanners used during fingerprinting could cause dangerous exposure to ultraviolet light, lasers, or other high-energy forms of light. If the US government implemented a biometric security program, government officials would have to develop a plan to educate the public on the need for such a program, and the benign nature of the collection. The government would also have to assume responsibility for unforeseen injuries caused by biometric collection.

In addition to the concerns that some may have concerning the safety of biometric collection, many people in the US associate biometric collection with criminality (Woodard et al., 2001). In the US, law enforcement uses biometrics extensively to solve crimes. Many Americans are familiar with televisions shows such as "CSI" that highlight

the use of biometrics to solve crimes. In the US, law enforcement officials take the fingerprints and photos of suspected criminals when they are "booked" for crimes and store them in databases for use in both the current and future criminal investigations. Many talk shows and television courtroom dramas feature judges and attorneys who use DNA evidence to identify "dead beat" parents who refuse to pay child support. The US military uses the BAT to identify potential terrorists in hostile areas. It is understandable that many Americans associate the collection of biometric information with criminal activity. This stigmatization as described by the RAND group, serves as a serious hurdle to the increased use of biometrics (Woodard et al., 2001). If private citizens have not committed crimes, they may question why their biometric data should be stored along with that of known or suspected criminals.

Sanitation

Another concern that many may have concerning biometric collection is sanitation. How and how often are biometric instruments sanitized? Can technicians transfer infectious diseases while using the instruments? Though hygiene may seem to some, a minor concern, it deserves consideration. Some fingerprinting instruments, for example, require that the subject place his or her hand on the instrument to allow the technician to capture the biometric. If technicians do not properly sanitize the equipment following each use, there is a risk that both subjects and technicians may suffer exposure to disease. The Transportation Security Administration (TSA) recognized that the spread of disease through physical contact with others and their personal items is a serious concern (Transportation Security Administration 2008). It is not uncommon to see gloved TSA agents rummaging through the personal effects of travelers prior to them

boarding a plane. According to their web site, the agents wear the gloves to prevent the spread of disease; however, it is not uncommon to witness TSA agents inspect multiple peoples' baggage without changing their gloves, thus protecting themselves from infection, but possibly exposing others to pathogens. TSA allows travelers to demand that the agent change gloves prior to checking their luggage in an effort to prevent the spread of disease (Transportation Security Administration 2008). The use of biometric devices raises a similar question. If physical contact is required to collect the biometric, then the potential spread of disease may require address. One must also consider, however, that having several people touch a biometric device may be no less sanitary that using a doorknob.

Informational Privacy

According to the RAND group, the most commonly held concern with the use of biometrics is associated with informational privacy. These concerns fall into three general categories: function creep, identity theft, and the tracking of individuals' activities (Woodard et al., 2001). Function creep in terms of biometrics is the use of a biometric for uses other than those stated at the time of collection. A company, for example may inform its employees that it intends to take a biometric sample to control access to a building, but later, the company may begin to use the biometric as a method of keeping timecards. Over time, additional functionality "creeps" into the system. The function creep involving the use of the social security number is illustrative of this point.

The Social Security Act (Public Law 74-271) established a number associated with taxes paid by private citizens to fund the retirement and survivor benefit programs managed by the Social Security Board (SSB). The Internal Revenue Service (IRS)

received a mandate to collect the taxes. To track the payment of such taxes, the SSB assigned a number to the tax payers, known as the social security number (SSN). In the following year, the SSB extended the use of the SSN to provide a tracking number for state unemployment insurance benefits. In 1943, Executive Order 9397 authorized the use of the SSN to identify all federal employees. Today, the number of uses of the SSN is astounding. The federal government, credit reporting agencies, financial institutions, educational institutions, and numerous other individuals and agencies use the SSN to identify personnel for various purposes (Electronic Privacy Information Center 2008). The function creep associated with the use of the SSN is primarily due to convenience. Unlike names, SSNs are unique identifiers. There may be multiple people with the same name, but the SSN applies to a specific person. The convenience that led to function creep associated with the SSN is expected with the use of biometrics.

Closely associated with the use of biometrics is the crime of identity theft. Identity theft, as described by the Federal Trade Commission (FTC), occurs when someone illegally uses another's personally identifying information, such as a name, SSN, or credit card number, without the individual's permission, to commit fraud or other crimes in the name of the victim (Federal Trade Commission 2008).

According to FTC statistics, as many as 9 million Americans suffer from identity theft each year. The use of a universal identification system enhances criminals' ability to steal identities (Federal Trade Commission 2008). When a criminal steals the name and SSN of an American citizen, he/she can use that information to access personal data, which allows the criminal to use the victim's credit, make purchases, secure loans, obtain health care, and perform a number of other illegal tasks in the name of the victim. The

Social Security Administration makes provisions to change individual SSNs for reasonable cause; however, it is difficult for the victim to recover completely from the theft of his/her identity. Theft of one's biometric information could potentially be much more disastrous. Unlike the SSN, biometrics cannot be altered; they remain relatively stable throughout one's life, and no agency can issue new biometrics to erase the consequences of identity theft.

The applications for the use of the SSN have grown significantly over time, and the trend will not likely change. The convenient use of a single identifier is attractive to many bureaucracies. If used appropriately, it allows access to a significant amount of information concerning a person that assists in the accurate accounting of taxes, decisions concerning employment, access to health care, extension of credit, and others. Biometrics will undoubtedly simplify many bureaucracies; however, the function creep that has plagued the use of the SSN will likely create concerns.

Religious Objections

Many fear the possibility of an insidious form of function creep. Some fundamentalist Christian groups fear that the use of biometrics fulfills a biblical prophecy of the "Mark of the Beast" (Woodard et al., 2001). Though some may dismiss this argument, many Christians believe that the book of Revelation predicted the development of biometric identification systems. "He also forced everyone, small and great, rich and poor, free and slave, to receive a mark on his right hand or on his forehead" (Revelation 13:16 (New International Version)). These people may believe that the purpose of biometric collection is to identify people as part of an effort made by an evil force to identify and segregate Christians from the general population with the goal of oppressing

them. The increasing use of various methods to identify people through the use of biometrics, social security numbers, credit cards, and other media fuels this sentiment.

> A third angel followed them and said in a loud voice: If anyone worships the beast and his image and receives his mark on the forehead or on the hand,
>
> he, too, will drink of the wine of God's fury, which has been poured full strength into the cup of his wrath. He will be tormented with burning sulphur in the presence of the holy angels and of the Lamb.
>
> And the smoke of their torment rises for ever and ever. There is no rest day or night for those who worship the beast and his image, or for anyone who receives the mark of his name. (Revelation 14:9-11 (NIV))

The passage above suggests that God will punish all who receive the "Mark of the Beast." This creates significant fear in those who believe in this construct. They have a deep fear that submission to biometric collection will cause God to punish them by eternal separation from Him in hell.

Anti-Government and Militia Groups

Finally, a number of Anti-government and militia groups tend to the reject the government's intervention in any areas of their lives. According to the Anti Defamation League, members of "patriot" organizations, such as the Militia of Montana have attempted to rescind or revoke their own driver's licenses or SSNs in an effort to preserve their anonymity (Anti-Defamation League 2007). Groups such as these believe that individual US citizens remain in a "sovereign" status until they enter into contractual agreements with the government. They use this reasoning to avoid some of the basic responsibilities of citizenship such as paying taxes and child support. They would likely believe that biometric collection interferes with their right to privacy, or constitute a "contract" with the government, which creates a fear that biometric data stored in various

databases will allow the government or other entities to track their behavior or otherwise limit their freedoms (Woodard et al., 2001) creating the Orwellian society described in *1984* (Orwell 1949). Their obsession with anonymity would make them highly unlikely to provide biometric samples to government organizations for any reason.

Constitutional Rights

The US Constitution protects American citizens' right to privacy and due process, and prevents its citizens from unreasonable search and seizure. The Fourth, Fifth, and Fourteenth Amendments codify these rights:

> Fourth Amendment
> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated; and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched and the persons or things to be seized.
>
> Fifth Amendment
> Any person shall be held to answer for a capital, or otherwise infamous, crime, unless on a presentment or indictment of a grand jury, except in cases arising in the land or naval forces, or in the militia, when in actual service, in time of war, or public danger; nor shall any person be subject, for the same offense to be twice put in jeopardy of life or limb; **nor shall any person be compelled, in any criminal case, to be a witness against himself, nor be deprived of life, liberty or property, without due process of law**; nor shall private property be taken for public use, without just compensation.
>
> Fourteenth Amendment
> Section 1. All persons born or naturalized in the United States, and subject to the jurisdiction thereof, are citizens of the United States and of the State wherein they reside. No State shall make or enforce any law, which shall abridge the privileges or immunities of citizens of the United States; **nor shall any State deprive any person of life, liberty, or property, without due process of law**, nor deny any person within its jurisdiction the equal protection of the laws.

In order to be effective in the prevention of terrorist activities, collection, storage, retrieval, and use of biometric information must meet constitutional standards and adhere

to public law. The next chapter discusses the laws and constitutional amendments that apply to biometric technologies when used to collection information from US citizens. It suggests possible methods that the US government may use to use biometrics as part of a comprehensive security plan while taking due consideration of the laws and constitutional amendments that protect the rights of US citizens.

CHAPTER 3

RESEARCH METHODOLOGY

Overview

The last chapter discussed the enormous body of research regarding biometrics. A great deal of research concerning the different biometric technologies is available; however, research concerning its legal implications is limited. Since the purpose of this research is to determine how to overcome legal challenges associated with the use of biotechnology, it is necessary to develop a methodology to analyze various courses of action (COA) that allow for the use of biometrics to identify US citizens without unduly infringing upon their rights. Various laws and constitutional amendments apply to the use of biometrics in the US. This chapter presents these laws and amendments as criteria to assess the suitability of various COAs the US government may take to integrate biometric technologies into a strategy that both improves security and protects the rights of US citizens.

Biometrics and the Constitution

When the Constitution does not specifically address an issue, courts use case law as a means of interpretation. In cases such as these, the judiciary establishes legal precedents. The Constitution does not address the use of biometrics directly; however, the Fourth Amendment protects US citizens from unreasonable searches and seizures. Courts often use this amendment to clarify individual rights when presented with cases involving the collection of physiologically based evidence such as fingerprints or blood. The Fourth Amendment states:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated; and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched and the persons or things to be seized.

In order to analyze the use of biometrics in terms of the Fourth Amendment, one must first ask the question: Does the taking of a biometric sample constitute a search? Many courts would likely agree that biometric collection does constitute a search. Many courts issued legal opinions associated with similar methods and technologies such as fingerprinting or drug testing. Davis v. Mississippi, 394 U.S. 721, 727 (1969), a case involving the use of fingerprints to convict an individual of rape, established that fingerprinting does constitute a search. Skinner v. Railway Labor Executives' Assn., 489 U.S. 602, 617 (1989), a case involving the use of urinalyses as a method of identifying personnel engaging in illicit drug use, established drug testing as a search under the Fourth Amendment. In National Treasury Employees Union v. Von Raab, 489 U.S. 656 (1989), the court ruled that it was legal to conduct drug testing on government employees with or without suspicion of illegal drug use. Such "suspicion less" searches may link individuals to criminal acts as determined by Michigan v. Sitz, 496 U.S. 444 (1990), the landmark case that confirmed the legality of sobriety checkpoints. As stated previously, courts use case law to interpret the Constitution and existing laws. Since the courts consider both fingerprinting and drug testing to constitute searches, it is likely that they will treat other physiologically based collections, such as biometrics similarly.

Since taking a biometric sample does constitute a search, one must then ask if the search is reasonable. If taking the sample is unreasonable, then it is in violation of the Fourth Amendment. The legal opinion associated with Davis v. Mississippi, 394 U.S.

721, 727 (1969), the case mentioned previously, determined that the collection of fingerprints did not constitute an unreasonable search. This legal opinion pertains to the taking of fingerprints from properly detained persons. Law enforcement officials routinely take fingerprints from detained individuals in the course of criminal investigations. It seems reasonable the courts may use this, and similar legal opinions, to allow the taking of biometric evidence other than fingerprints, from lawfully detained persons. Though this ruling may address the collection of biometric evidence from properly detained personnel, it does not apply to "free persons."

With regard to free persons, in Katz v. United States, 389 U.S. 347 (1967), the Supreme Court clarified that the Fourth Amendment protects people, not places. Therefore, wherever a person has a reasonable expectation of privacy he/she is entitled to be free from unreasonable government intrusion. This legal opinion, however, does not guarantee the absolute right to privacy to free persons. There are a number of examples where the government offsets citizens' fourth amendment rights when it is in the interest of public safety. Certain elements of the Patriot Act, discussed later in this chapter, address this issue.

Collecting biometric samples from detained personnel is an established lawful practice. When devising a strategy that involves the collection of biometric information from free persons, government officials must consider the individual's right to privacy, and ensure that the collection does not constitute an unreasonable search. An overarching strategy should allow for biometric collection from as many people as possible to create as wide a pool of biometric data as possible. This establishes the first criteria considered

when incorporating biometrics into a security strategy. The program must take into consideration individual privacy and avoid the use of unreasonable searches and seizures.

A second Constitutional Amendment that pertains to the use of biometrics is the Fifth Amendment, which protects individuals from self-incrimination. The verbiage of the Fifth Amendment follows:

> Any person shall be held to answer for a capital, or otherwise infamous, crime, unless on a presentment or indictment of a grand jury, except in cases arising in the land or naval forces, or in the militia, when in actual service, in time of war, or public danger; nor shall any person be subject, for the same offense to be twice put in jeopardy of life or limb; nor shall any person be compelled , in any criminal case, to be a witness against himself, nor be deprived of life, liberty or property, without due process of law; nor shall private property be taken for public use, without just compensation.

The Fifth Amendment raises an interesting question to those who might collect biometric data for the purpose of law enforcement. Can law enforcement prosecute an individual for a crime based on biometric data collected for other than criminal reasons? In the case of Breithaupt v. Abram, 352 U.S. 432 (1957), the court ruled that blood samples taken from an unconscious defendant were admissible as evidence because the taking of blood is non-intrusive, and therefore does not violate privacy rights. What appears to be the litmus test in this case is the level of intrusion involved in taking the biometric; therefore, in order to ensure that biometric information in databases meet the standard for criminal prosecution, the method of taking the biometric must be as unobtrusive as possible. The court also determined in the case of Perkey v. Department of Motor Vehicles (1986) 42 Cal. 3d. 185, that since fingerprinting occurs without penetrating the skin, the use of fingerprinting in criminal procedures is acceptable, and does not violate one's right to privacy. Though fingerprinting does not involve penetrating the skin, other biometrics may not meet that standard. In one case, Rochin v.

California, 342 U.S. 165 (1953), the court ruled that evidence gained during an involuntary stomach pumping was inadmissible due to the shocking method of obtaining the evidence as well as the level of intrusiveness involved in pumping one's stomach.

The courts agree that the unobtrusive collection of fingerprints and their use in criminal proceedings does not violate Fifth Amendment rights. Since the court determined fingerprinting, since it does not penetrate the skin, to be unobtrusive, it would likely expand this standard to the use of other biometric collection methods that do not involve the penetration of the skin. Though the court's opinion that the taking of blood is also unobtrusive does allow for the possible incorporation of more intrusive methods of biometric sampling, it is difficult to determine the level at which physiological sampling becomes intrusive enough to cause courts to rule it in violation of Fifth Amendment rights. It is therefore more advantageous to gear biometric collection to the less obtrusive criterion of using methods that do not penetrate the skin. This establishes a second criterion used for the incorporation of biometrics into a security strategy. The system used for biometric collection should collect the biometric without penetrating the skin.

A third Constitutional Amendment, the Fourteenth Amendment also applies to biometric collection techniques. The Fourteenth Amendment guarantees US citizens the right to due process. Section One of the Fourteenth Amendment clearly establishes this right:

> All persons born or naturalized in the United States, and subject to the jurisdiction thereof, are citizens of the United States and of the State wherein they reside. No State shall make or enforce any law, which shall abridge the privileges or immunities of citizens of the United States; nor shall any State deprive any person of life, liberty, or property, without due process of law, nor deny any person within its jurisdiction the equal protection of the laws.

The Fourteenth Amendment of the Constitution requires the government to enforce laws and policies in such a way that they do not violate the rights of US citizens. If the government must violate the rights of an eligible individual, it must first present a compelling reason for having done so, and it must provide an appeals process through which the individual may respond to the intrusion. The government normally presents its case for intruding upon the rights of its citizens through either a pretemination or a predetermination hearing prior to suspending or revoking the privilege.

The court, during the pretemination or predetermination hearing, first must determine whether or not the violation of due process serves the public interest to the degree that the value of the information gathered as a result of the collection outweighs the protection of individual rights. In order to make this determination, the court must know the purpose of the action. If the court determines that the purpose of the action is vital to the interest of the public, then it may override the individual's rights (Understanding Privacy Laws 2007). This often occurs during the process of criminal investigations, in cases where the health or safety of the public is at risk, or in the case that the collection of the information is vital to the security of the nation. In the case of Cafeteria Workers v. McElroy, 367 U.S. 886 (1961), the Supreme Court determined that it would allow the firing of a cafeteria worker, who worked in a secure government facility because she did not pass a security background check. In this case, the court determined that the presence of individual who failed to meet the security requirements to work in the government facility would compromise the security infrastructure of the building, and possibly breach national security. In this case, the interest of national security outweighed the rights of the individual.

One could argue that the security of the nation is at risk due to the threat of international terrorism; however, it is not likely that courts would allow the government to collect biometric information from all US citizens as part of a security program. Since terrorists probably represent a very small percentage of Americans, it would not be appropriate to override the rights of all Americans to capture a few terrorists. One method to ensure the government does not violate the individual's right to due process is to institute a program that requires informed consent from the individual. This presents a third criterion to consider when developing a security program that integrates biometric collection. The government must inform citizens of the purpose of the biometric collection, and obtain individual consent prior to collection.

Biometric tools have powerful implications for the GWOT and for law enforcement in general. Properly employed, biometrics may positively identify criminals and other terrorists and greatly improve the security of the nation. Like any other technology, however, it is not perfect. Incorrect biometric matching may incriminate innocent people. This is compounded by what may be known as the "CSI Effect" (CSI Effect 2007), a phenomenon that many lawyers claim describes the attitude that many jurors now have toward the presentation of forensic evidence such a biometrics in court proceedings that causes them to put an inordinate amount of trust in biometrics and other forensic evidence. The CSI Effect, named for the television show that highlights the use of forensic evidence in court proceedings, may cause jurors to assume that any forensic evidence, to include biometrics, always determines innocence or guilt. Though there is some debate over the power that the CSI Effect has over jurors, it is clear that such an attitude could cause infringement on the individual's right to due process.

Biometrics and Congressional Legislation

In addition to the Constitutional Amendments associated with the use of biometrics, one must consider Congressional legislation designed to strengthen the security of the nation following the terrorist attacks on September 11, 2001. Chief among these laws is the Patriot Act. The US Congress passed Public Law 107-56, Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism, also known as the Patriot Act, which authorized US government agencies to take extraordinary measures designed to combat the threat of both domestic and international terrorism following the September 11, 2001 terrorist attacks against the US. The Patriot Act directed the Attorney General and the National Institute of Standards and Technology (NIST) to develop biometric identifier standards that "can be used to verify the identity of persons applying for a US visa or such persons seeking to enter the US pursuant to a visa for the purposes of conducting background checks, confirming identity, and ensuring that a person has not received a visa under a different name." In response to the Patriot Act, NIST, and other government agencies began to develop and to contract the development of biometric technologies to prosecute the GWOT. This directive established the need for biometric collection as a tool to assist in this endeavor.

The Patriot Act seeks to identify persons who desire to enter the US by performing background checks on foreign passport holders and visa candidates to ensure individuals do not attempt to enter the US using fraudulent visas. The addition of biometric markers increases the effectiveness of the program by fixing the name of the individual on the passport with a biometric. By fixing the individual's identity to the

passport, border patrol agents may identify persons who attempt to enter the US using multiple names or multiple visas. It also allows the government to maintain databases that record biometric and personal information concerning visitors to the US. This database assists law enforcement personnel in the identification of suspected terrorists and other criminals. If, for example, an individual enters the US and robs a convenience store, leaving behind his latent fingerprints, law enforcement personnel may collect the latent fingerprints and compare them to fingerprints in the databases to identify the culprits.

US citizens would likely oppose the implementation of any strategy that demands that every citizen submits his biometric data to the government for inclusion in databases used to identify terrorists and other criminals. Such a program would violate the individual's right to privacy without providing a compelling reason for doing so.

The Patriot Act also gave the US government the authority to delay notice of the execution of a warrant. This delay in the issuance of a warrant establishes the right of the US government to "delay with respect to the issuance of any warrant or court order under this section, or any other rule of law, to search for and seize any property or material that constitutes evidence of a criminal offense in violation of the laws of the United States, any notice required, or that may be required, to be given may be delayed if (1) the court finds reasonable cause to believe that providing immediate notification of the execution of the warrant may have an adverse result, (2) the warrant prohibits the seizure of any tangible property, any wire or electronic communication, any stored wire or electronic information, except where the court finds reasonable necessity for the seizure; and (3) the warrant provides for the giving of such notice within a reasonable period of its execution,

which period may thereafter be extended by the court for good cause shown." This section of the Patriot Act gives the government a great deal of latitude concerning suspending citizens' right to due process in the interest of national security.

The purpose of the Patriot Act is to provide the government increased latitude in the methods that it uses to prosecute the GWOT. It establishes the use of biometric applications to assist in the protection of the US borders against terrorists. Though its implementation does not place significant limits on the use of biometrics as part of a comprehensive security strategy, it does establish the need for biometric technologies to identify persons seeking US visas, or seeking entry into the US using a passport. This presents a fourth criterion. A biometric security strategy should assist in identifying personnel in the interest of prosecuting the GWOT.

Though the Patriot Act increases government powers to prosecute the GWOT, government officials must consider the provisions of the Privacy Act, and make every effort to protect the privacy of US citizens. The Privacy Act of 1974 regulates the government's maintenance, collection, and distribution of personal information. It seeks to protect personal information held by government agencies through the establishment of safeguards to prevent the theft or abuse of records. It requires government agencies to keep accurate personal records, allow individuals access to their personal records, and to provide means by which individuals may correct their records in the event that information appearing in the record is incorrect. Finally, it restricts government agencies from disclosing personal information.

The Privacy Act does not specifically address the collection and storage of biometric information, but it does address personal information in terms of records. Title

5, US Code, Chapter 5 defines a record as “any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.” It further defines a system of records as “a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.” It is likely that the definitions of records and systems of records as defined by Title 5 would apply to biometric records and databases.

The use of biometric records and databases raises a number of privacy concerns. A major concern involves the accuracy of the record. The Privacy Act guarantees individuals the right to review and correct their records; however, this becomes problematic with a biometric record. It is difficult to verify the accuracy of visible biometrics such as fingerprints, and it is significantly more difficult to verify the accuracy of one’s retinal scan, or DNA sample. The federal government charged NIST with the responsibility of establishing standards for the collection of biometrics (Wilson 2004), but did not present the organization with the task of correcting and verifying individual records. During the process of a criminal investigation, incorrect biometric information in databases could lead to the arrest and detention of innocent persons or allow guilty individuals to avoid capture. This leads some criminals to alter their biometrics to avoid arrest.

Associated with the difficulty of identifying inaccuracies in a record is the possibility of the theft of a record. Identity theft is currently on the rise given the unprecedented access to information associated with the use of computerized data. The US government acknowledges the theft of information from several government databases protected under the Privacy Act, to include the theft of information from two Veterans Administration (VA) databases (USA.gov 2007). The stolen databases included a significant amount of personal information, which criminals could use to steal identities. The government provides remedies for those affected by identity theft. In extreme cases, the Social Security Administration may issue the identity theft victim a new social security number (Social Security Administration 2007). The theft of biometric information would present a significantly more challenging problem. An individual may change information such as a name or a social security number, but he cannot change biometric information in response to biometric identity theft. As the government develops a more robust biometric capability, it must provide some remedy for victims of biometric identity theft. The government must also take significant security measures to protect the databases not only from those who would steal biometric information, but also from those who would seek to alter the databases for criminal reasons. This presents a fifth criterion: a biometric security strategy should protect personal information in accordance with the Privacy Act.

In summary, an acceptable biometric strategy should consider the individual's right to privacy, and ensure that the collection does not constitute an unreasonable search, allow the collection of biometrics without penetrating the skin, inform citizens of the purpose of the biometric collection, obtain individual consent prior to the collection,

assist in identifying personnel in the interest of prosecuting the GWOT, and protect personal information in accordance with the Privacy Act.

Courses of Action

US government agencies use biometrics in a variety of different ways; however, no strategy used to date seems to harness the immense power of the tools to form a strategy that protects the rights of US citizens while protecting the homeland. The following COAs represent three strategies that the US government may employ to effectively use biometrics the homeland while protecting the rights of US citizens:

COA 1: Mandatory biometric collection against all persons within US sovereign territory. This COA would mandate that all persons within sovereign US territories submit to mandatory biometric sampling. The government would maintain digital representations of individual biometrics in secure databases accessible to all law enforcement agencies to assist them in the arrest, detention, and prosecution of known or suspected terrorists and other criminals.

COA 2: Mandatory biometric collection against properly detained personnel, while merging existing government criminal databases to form master data network used by law enforcement to prosecute the GWOT.

This COA is already in effect to some degree. Many law enforcement officials routinely collect DNA, fingerprints and photos from properly detained personnel. It would mandate that all law enforcement organizations collect specified biometrics from all properly detained personnel. In addition to the mandatory collection of select biometrics against properly detained personnel, government agencies would develop interactive and compatible databases that may query all government biometric databases

to assist law enforcement agencies in the arrest, detention, and prosecution of known or suspected criminals.

COA 3: Biometric collection in conjunction with privileges associated with US citizenship. This COA would link the collection of biometric information by government agencies to privileges associated with US citizenship such as obtaining a birth certificate, driver's license, passport, or voter's registration card. In order to receive the benefits of full citizenship, on would have to submit to biometric sampling. Refusal to provide biometrics would prevent the party from obtaining specified benefits. The government would maintain digital representations of individual biometrics in secure databases accessible to law enforcement agencies to assist them in the arrest, detention, and prosecution of known or suspected criminals.

The next chapter analyzes each of the presented COAs in terms of their feasibility, suitability, and acceptability in an effort of choose the most viable COA that the US government may take to harness the immense power of biometrics to identify known or suspected terrorists and other criminals to assist in the prosecution of the GWOT.

CHAPTER 4

ANALYSIS

Introduction

The last chapter discussed some of the Constitutional Amendments and laws associated with the use of biometrics and presented COAs that the US government might pursue to increase the effectiveness of security plans using biometrics. This chapter presents an acceptable model for biometric collection and an analysis of the COAs presented in chapter 3 with the intent of selecting a COA that best suits the needs of the federal government, and takes appropriate consideration of the rights of US citizens as dictated by law and the US Constitution.

The BAT: An Acceptable Biometric Collection Device

An acceptable model for biometric collection is already in use by the DoD. The BAT, introduced in chapter 2, collects three biometrics for storage into databases that military or law enforcement personnel may query to assist in the identification of personnel. The three biometrics collected are digital photos, digitized fingerprints, and iris scans (Onley 2004). The BAT or a similar system, would serve as an effective tool for the US government to positively identify personnel. Biometric technicians could easily operate the system in a public environment, eliminating the possibility of violating Fourth Amendment rights. It collects biometrics without penetrating the skin, so it is unlikely that the collection method would violate Fifth Amendment rights. The US government would have to establish protocols for obtaining individual consent for biometric collection, and inform individuals of the possible future applications of the

information to ensure the right to due process. The US government would also be required to emplace adequate safeguards to protect the biometric databases from compromise or abuse, and finally, use those databases as tools to compare biometrics from various sources as part of a strategy to identify terrorists and other criminals in support of the GWOT.

Since the BAT is presently in use by the DoD, and has demonstrated a high degree of effectiveness, it should be adopted by all interested US government agencies. This would reduce the research and development costs associated with developing new systems, as well as ensure the interoperability of systems, allowing DoD and other government agencies to easily search multiple databases for biometric matches. Periodic modification of the systems would be necessary; however, the basic protocol should remain the same. Since the components of the BAT are commercial off the shelf (COF) products, they are readily available, and require only minor modification for government use. The government would also benefit from emerging technologies in the private sector that may increase the efficiency of a BAT-type system, allowing for the upgrade of equipment to ensure that it incorporates the most recent and effective technologies.

Multiple federal and state agencies use biometric tools to identify personnel; however, the systems are not completely interoperable. The Intelligence Reform and Terrorism Prevention Act of 2004 requires the creation of an "information sharing environment to share terrorism information across the homeland security, law enforcement, and intelligence communities at all levels of government and the private sector, and accelerated development of an integrated electronic biometric entry-exit screening system" (Global Security.org 2007). Despite the fact that this law seems to

mandate that the systems used by US government agencies are compatible, various branches of the government continue to operate using systems that are not fully compatible with each other.

The Automated Biometric Identification System (IDENT), used by the Immigration and Naturalization Service (INS) and IAFIS, used by the FBI, both collect ten flat digitally scanned fingerprints to ensure compatibility of biometric templates. This allows the US Border Patrol to digitally scan fingerprints of persons attempting to enter US borders, and send the digital prints to the FBI for identification (Global Security.org 2007). Prior to the assumption of similar fingerprinting formats, the Border Patrol agents collected only two fingerprints from personnel requesting entry into the US (Amerson 2007). The IAFIS database stored ten fingerprint samples, which made the two systems only marginally compatible. In many cases, Border Patrol agents would wait for days, and sometimes months for the FBI to analyze fingerprints. Now that both organizations operate on a single platform, Border Patrol agents may search the IAFIS database for possible fingerprint matches in a few hours (Global Security.org 2007).

The improvement in timeliness is not only due to the use of a single format, but it can also be attributed to the automation of fingerprint profiles, which allows for on-line searching of databases, which resolves the issue of slow throughput that plagued the previous system. The USCG, however, has not yet adopted a ten-print template for biometric collection. The process that the USCG uses to match fingerprints within the IAFIS database takes longer than the process used by INS, however, this does not currently present a problem for the USCG because of the relatively small number of personnel caught attempting to illegally immigrate to the US via the Mona Pass. The

lack of complete compatibility with IAFIS may eventually cause serious problems within the USCG program as it expands the program from the Mona Pass to other well-known illegal immigrant maritime routes. The number of personnel detained at sea due to suspected illegal immigration may eventually demand, based on the USCG's inability to detain personnel on cutter indefinitely, that the USCG adopt a ten-digital fingerprint platform to increase compatibility with existing databases to improve throughput (Amerson 2007).

The adoption of a single BAT-type system would not only ensure compatibility of systems and increase the speed of biometric matching, but it would also increase accuracy in identification. Unfortunately, biometrics are not always unique. There have been a few isolated cases where identical twins presented some identical biometrics. Additionally, no system is perfect. In some cases, instead of retrieving a single match for a fingerprint, IAFIS produces a number of potential matches (Fingerprint Identification Systems, 2008). A system that incorporates the use of multiple biometrics would be preferable to one that uses only one because it is highly unlikely that two people share multiple biometrics.

Using the BAT or a similar technology platform, the DHS and other government agencies may choose among several COAs for its implementation in support of the GWOT. The following section analyzes each COA presented in chapter 3 in terms of its feasibility, applicability and suitability.

COA 1-Mandatory Biometric Collection Against all Persons within US Sovereign Territory

As stated in chapter 3, this COA would mandate that all persons within sovereign US territories submit to mandatory biometric collection. A designated government agency would maintain digital representations of specified individual biometrics in secure databases accessible to law enforcement agencies to assist them in the arrest, detention, and prosecution of known or suspected criminals.

Feasibility

The US government possesses the appropriate technology to implement a comprehensive biometric program. As stated previously, the BAT provides the US government with a powerful tool to identify personnel. It is possible to field enough systems to the appropriate government agencies to maximize biometric collection; however, the US government would have to determine how and when the collection would take place. The infrastructure to collect biometrics upon entry and exit from the US exists. The US government would have to field BAT-type systems to the INS, USCG, and other agencies that control the US borders, as well as other agencies that the US government would designate to serve as biometric collection agencies. The government would establish a protocol for the collection, storage, and retrieval of biometric information and store it as dictated by the Privacy Act. Fielding of the systems as well as providing the support infrastructure to ensure that the systems remain operational would probably be cost-prohibitive. In this case, it may be preferable to focus on high risk groups that the US government believes may produce or harbor terrorists. It would be very difficult to justify the expenditure of US government funds to

support a program that primarily targets innocent civilians as part of a strategy to prosecute the GWOT.

Applicability

This is an attractive COA for government and law enforcement officials because it would allow for the creation of a comprehensive database, which law enforcement personnel may query as part of official investigations. Such a system would allow law enforcement officials to collect biometrics seized at crime scenes, and query the databases to obtain a list of possible suspects. This would greatly reduce the time required to conduct criminal investigations where the offender leaves latent biometrics. In the case of a terrorist attack, law enforcement officials would collect biometric information from the scene of the attack and enter it into a software program that would compare the biometrics left at the site to biometrics of all persons in the US to assist in the identification of the attacker. The system would produce a list of possible perpetrators, allowing law enforcement officials to focus on the location and detention of a select group of people.

The USVISIT/IDENT systems require biometric sampling of all persons entering and exiting the US (Global Security.org 2007). These databases, as previously discussed, interact with the FBI's IAFIS system to determine the identity of personnel. The interaction with IAFIS also alerts government officials at entry and exit points in the US of the criminal history associated with the biometric. Enacting a comprehensive biometrics collection program using multiple biometrics for all persons within US territories would create a vast database that US government personnel may query for official reasons. Unless a criminal entered the US illegal through a porous, unmonitored

border, his biometrics would theoretically be available to US government officials. Not only does this serve to remove the terrorist's cloak of anonymity, but also it removes the cloak of anonymity from previously detained criminals who leave biometrics at the scene of a crime. Local police and other qualified agents would simply have to find biometrics left at the scene of the crime and compare them to those in the databases to generate a list of probable subjects.

Suitability

Though this seems an attractive option, the government must consider individual rights as set forth by law and the US Constitution. To determine the suitability of such a program, one would have to consider the law and Constitutional Amendments discussed in chapter 3, namely the Fourth, Fifth, and Fourteenth Amendments as well as the Privacy Act and the Patriot Act.

Chapter 3 discusses the Fourth Amendment of the US Constitution as it applies to biometrics. The Fourth Amendment protects US citizens from unreasonable search and seizure. Case law, as presented in chapter 2, determined that biometric collection constitutes a seizure; however, it would not normally be considered an unreasonable seizure. In this case, however, the seizure may be unreasonable. No US government entity has an established reason for requiring all citizens of the US to submit to biometric collection. One might argue that the protection of the US and its interests may require that the government and law enforcement agencies receive extraordinary powers as dictated by the Patriot Act or similar legislation to enact such measures; however, the need for internal security must be balanced with the right of individual privacy. It is unlikely that the government would receive the latitude to invade the privacy of all its

citizens if the goal is to identify only a small number of people. Additionally, the government would have to develop comprehensive security systems to protect the biometric data.

The federal government has, in a number of cases, failed to provide adequate protection for individual records as required by the Privacy Act. These failures in security led to the compromise of personal information regarding military and other personnel that could potentially lead to identity theft. The specter of identity theft has come to the forefront due to the unprecedented access to computer records and databases containing personal information kept by government agencies and private companies. As stated in chapter 2, under extreme cases, the SSA may issue a victim of identity theft a new SSN; however, since biometrics involves the collection of physiologically based records, they are irreplaceable. Theft of biometric information could be catastrophic to the victim.

In addition to protection from the invasion of privacy, through the Fifth Amendment, citizens have the right to avoid self-incrimination. This issue could be addressed by requiring mandatory consent prior to biometric collection; however, since the collection would be mandatory, it is likely that a conviction based on biometric evidence obtained from a person who did not provide express consent would be dismissed in court.

Though this COA does not seem suitable for use in the US, it is used extensively in both Afghanistan and Iraq where military personnel routinely collect iris scans, digital photos, and fingerprints from the Afghans and Iraqis in an effort to locate and detain known and suspected terrorists (Onley 2004). The US military primarily uses two

systems to collect biometrics known as the Biometric Automated Toolkit (BAT) and the Hand-Held Interagency Identity Detection Device (HIIDE). The BAT, as stated in chapter 1, is a portable system consisting of a laptop computer, a digital camera, and a fingerprint scanner. The BAT collects biometric information from the Afghans and Iraqis, to verify their identities and to locate and detain known and suspected terrorists. It also produces identification cards with digital representations of biometrics embedded in the card. The use of such an ID card assists in access control at border crossings, checkpoints, and security control points. The BAT stores digital photos, fingerprints, and iris scans and uploads them into a central database. Once an individual's biometrics are loaded into the BAT, the system conducts a "one to many" search of the database to determine if the individual's biometrics were previously enrolled. If his biometrics do not appear in the database, the subject is immediately enrolled, and his biometrics are entered into the database. This allows the user to identify any person previously enrolled in the database, and allows for the enrollment of new personnel (Woodard 2005).

The BAT database uses compartments to separate records of regular citizens from the records of known or suspected terrorists and other criminals. This feature allows for the identification and detention of known or suspected terrorists and other criminals while recording personal information of average citizens. In addition to these features, the BAT allows for the storage of biometric information of unknown personnel. This feature is attractive because it allows investigators at crime scenes to collect biometrics from the scene and store them in a database. In the event that the biometrics collected at the scene match those of someone who is enrolled in the system, then the investigator can obtain the identity of the suspect. If the biometrics do not exist in the database, then the

information remains active in the database until someone with matching biometrics is enrolled in the system. This allows for the identification and detention of the suspect immediately upon enrollment (Woodard 2005).

The HIIDE is a smaller and more portable version of the BAT. The BAT requires the use of a laptop computer, so its use is not ideal in field conditions. The HIIDE is smaller and less cumbersome than the BAT, and is often taken with military squads on patrol. It is a palm-sized device that allows the user to collect digital photos, fingerprints, and iris scans in that same format used by the BAT. Though it cannot link directly into large biometric databases, users may download biometric information from terrorist, criminal, and other watch lists from a BAT to a HIIDE, and take the HIIDE on patrol. The HIIDE has the same biometric comparison capability as the BAT, only it uses a much smaller database. While on patrol, squad members collect biometrics from local personnel, enrolling those who do not already exist in the database, and confirming the identities of those who already exist in the database. This method of collecting and analyzing biometrics also allows the squad members to compare the local citizens' biometrics to those in terrorist, criminal, and other databases that are contained in the HIIDE. Once a squad returns from a patrol, they download the information from the HIIDE to the BAT so that any newly collected biometrics are loaded into the BAT database (Last Tactical Mile vs First Tactical Mile 2007).

The biometric collection programs in Afghanistan and Iraq are immensely successful, however such a strategy would not be appropriate for use with US citizens within the nation's borders due to it's incompatibility with the individual right to privacy. Without sufficient cause such as multiple massive terrorist attacks against the US

homeland, it is unlikely that US citizens would allow for the expansion of the provisions of the Patriot Act or the implementation of a similar law to mandate biometric collection against all persons in the US. A modification of this strategy as described in COA 2, however, may be appropriate for use in the US.

COA 2-Mandatory Biometric Collection Against Properly Detained Personnel, While Merging Existing Government Criminal Databases to form Master Data Networks Used by Law Enforcement to Prosecute the GWOT

Biometric collection against properly detained personnel is a common strategy used by law enforcement officials to record information concerning known and suspected criminals. Once an individual is properly arrested and detained, in many instances, he is compelled to submit to photographing, fingerprinting, and in some cases, DNA collection. Law enforcement agencies retain this information on file for use in criminal investigations. When law enforcement officials investigate crimes, they routinely query biometric databases to determine whether biometrics found at the scene of the crime match those of a known or suspected criminal within the database. The officials often use photos of known or suspected criminals as "line up" photos for victim review in connection with an investigation (Mrowka 1996). As stated previously, the US government currently maintains a number of biometric databases that contain physiological information collected from criminals. Mandating the collection of specified biometrics to populate all criminal databases, and configuring them to interact with each other to identify terrorists and other criminals would add increased functionality of this COA.

Feasibility

This COA seems ideal because it is similar to the methodology in use. It does not call into question individual rights because US citizens lose certain rights to privacy once properly detained. The interactive nature of the databases would allow for the creation of mass databases to query for information concerning known and suspected terrorists and other criminals. A drawback of this strategy is that not all law enforcement agencies exercise their right to collect biometrics against properly detained personnel. Additionally, there is no standard protocol in use for all law enforcement agencies. In order to maximize the effectiveness of the use of such a strategy, the federal government would have to mandate a specific protocol for the use of biometrics by law enforcement officials. This would include dictating the circumstances under which biometrics must be collected, the types of biometrics to be collected, and the format used for collection. This would ensure that all law enforcement agencies have the required technology to implement a biometric security program, using compatible databases. Interoperability is key in cases such as these because it allows for the comparison of biometrics in multiple databases to maximize the probability of matching the biometric in question. This would allow a police officer to detain an individual suspected of a crime, collect the individual's biometrics, and forward the biometrics to multiple government agencies for comparison against existing databases as part of an investigation. Such a program would link law enforcement and government agency investigative power, increasing the probability of solving crimes by maximizing the use of crime databases.

Suitability

The obvious shortfall in the use of this methodology, in the absence of interactive databases that capitalize on all government biometric records, is that the pool of biometric information would be severely limited considering that only the biometrics of known and suspected criminals exists in the database. Such a program would be beneficial in the identification of criminals who commit multiple crimes; however, it would not be very effective in identifying personnel who have no criminal history. It is likely that terrorist cells would counter government efforts by recruiting from pools of people with no criminal history. Without the interactive databases, COA 2 would probably result in the production of databases populated with primarily US citizens. This may be an acceptable strategy for use by local law enforcement agencies to combat local crime, however in the case of international terrorism; it is likely that perpetrators of the crime are not US citizens, and therefore would not exist in the criminal databases.

Applicability

A program that collects multiple biometrics from properly detained personnel in format that allows for interoperability of biometric matching programs would be of great value in the prosecution of the GWOT. Many terrorists and other criminals have criminal histories. Such a system would provide law enforcement officials with a powerful investigative tool to identify terrorists and other criminals. It fails, however, to provide a means to identify terrorists and other criminals with no criminal history or biometics on file.

Biometrics would not serve as a panacea for all law enforcement woes. One must remember that biometric information is not always unique. In the case of identical twins,

or other multiples originating from a single egg, biometrics may be indistinguishable because the genetics used to create the individuals were identical. The case below highlights this concern.

The Cooper Case

In November 1999, a man brutally raped a young female student attending Kendall College of Art and Design. Following the rape, the young woman reported the incident to local police in Grand Rapids, Michigan, and in keeping with investigative procedures, the woman received a sexual assault physical examination to collect physical evidence to assist in apprehension of the assailant. Medical personnel recovered physical evidence from the woman, to include the attacker's semen sample containing his DNA, and sent the sample to the state crime lab where law enforcement personnel store and analyze crime scene evidence (Willing 2004).

The crime went unsolved until 2003 when Jerome Cooper, a convicted felon held in a Michigan prison, applied for parole. In accordance with Michigan State law, all felons who apply for parole must first submit a DNA sample for analysis. The felon agrees to allow law enforcement personnel to compare his/her DNA to DNA recovered from unsolved crime scenes. Jerome Cooper's DNA perfectly matched that of the young rape victim. Investigators believed that they had identified the culprit, and were particularly relieved that the suspect, Jerome Cooper, was already in custody. Their jubilation ended abruptly when they discovered that Jerome Cooper had an identical twin brother, Tyrone Cooper (Willing 2004).

Why did this cause so much angst? Identical multiples births occur when an early embryonic division causes the development of more than one child. Since the division

occurs shortly after fertilization, the offspring possess identical DNA sequences, creating a serious problem for those who would desire to use DNA as the primary method of distinguishing one identical multiple from another. The investigation would not have taken such a grave turn if Tyrone and Jerome Cooper were fraternal twins. Since fraternal multiples develop from the fertilization of separate eggs, the offspring are no more genetically similar than any other siblings. To further complicate the issue, background investigations revealed that both Tyrone and Jerome Cooper had prior convictions for sexual assault (Willing 2004).

A Biotechnology company, Orchid Cellmark analyzed both twins' DNA in an effort to resolve the issue. They worked using the premise that DNA is prone to producing minor genetic mutations at birth and throughout life, causing the twins to show minor differences in DNA sequences. They planned to take DNA samples from both twins, and analyze it to find minor mutations that would allow them to distinguish between the twins' DNA. Once they located the mutations, and were able to distinguish between the two sets of DNA, they would compare the DNA recovered during the rape investigation to both twins' DNA to assign responsibility for the crime. This method seemed ingenious and quite promising; however, it did not produce the results expected. After exhausting all of their protocols, Orchid Cellmark was unable to distinguish between the two DNA samples (Willing 2004).

The Cooper case reveals some of the concerns raised by the use biometrics to resolve crimes. In rare cases, such as this one, biometrics are not unique. It is possible that the investigators could have identified the culprit if they had recovered more biometric evidence at the scene of the crime. If, for example, investigators had recovered

fingerprints from the crime scene in addition to the DNA, they could have used the DNA to narrow the number of suspects, and used the twins' fingerprints to confirm the identity of the attacker, or vice versa. In any case, the use of more than one biometric to identify personnel would tend to promote accuracy in identification. In the interest of protecting US citizens from false identification, a model system would collect more than one biometric to increase accuracy in identification.

This case demonstrates the need for due process in all cases involving biometric evidence. Many legal experts often describe the "CSI Effect," a term that describes the reliance that many jurors appear to place on forensic evidence as demonstrated by the popular television show "CSI." The television show highlights the use of forensic evidence such as biometrics to solve crimes. The CSI Effect causes many jurors to accept forensic evidence as being irrefutable in determining guilt or innocence. In cases such as these, where biometrics cannot accurately distinguish between people, the jurors, and others involved in the legal process, may unknowingly rob an individual of his right to due process. In order to protect the right to due process, the employment of a strategy that incorporates the use of multiple biometrics would be preferable to a strategy that uses only one. The use of multiple biometrics increases the probability of correct identification. In the Cooper case, for example, the brothers shared the same DNA information, but it is unlikely that they share the same fingerprints and the same DNA. If it were possible to analyze latent fingerprints in addition to the DNA samples, the court may have been able to correctly identify the culprit based on his DNA/fingerprint profile.

The Cooper Case magnifies a major shortfall associated with the implementation of COA 2 without the incorporation of the interactive databases. To address the issue

raised by the collection of similar biometrics from different people, COA 2 would best be modified by requiring law enforcement officials to collect more than one biometric from suspected criminals, as it is unlikely that two people share all of the same biometrics. As stated previously, this COA would primarily generate databases containing biometrics of criminals, limiting information on those potential terrorists who have either never committed a crime, or never been arrested in conjunction with a criminal investigation. COA 3, biometric collection in conjunction with privileges associated with US citizenship, which would mandate the collection of biometrics against most US citizens, may be of use to expand the information in biometrics databases to include a wider pool of people.

COA 3-Biometric Collection in Conjunction with Privileges Associated with US Citizenship.

In this case, the federal or local government would collect biometric information when US citizens apply for passports, pay taxes, request birth certificates, obtain driver's licenses, or any other government-issued credential. This COA would collect biometrics from most US citizens, as daily life in the US requires the use of government credentials. Associating a biometric with these credentials would allow for the collection of biometrics into a database for law enforcement personnel to search during criminal investigations. The database would be extremely valuable to law enforcement agencies as it provides officials a readily available database containing the biometrics of a majority of US personnel to assist in the resolution of criminal investigations.

This COA differs from that of mandatory biometric collection in that individuals may opt out of the program. The choice to opt out, however, would limit individual

access to many of the benefits of citizenship. A major concern s raised by the use of such a program is that many people would perceive the program to be identical to a program involving mandatory collection, as the government would refuse them access to many benefits of citizenship based on their refusal to submit to sampling.

Feasibility

The program would probably not violate the Fourth Amendment as the collection would be voluntary, and would therefore not constitute an unreasonable search and seizure. The government would have to implement extensive safeguards to prevent compromise of the database to insure the individual right to due process as dictated by the Privacy Act and the Fifth Amendment. The program would likely be challenged based on the Fourteenth Amendment, as to many, it would appear that the government is depriving citizens of the US certain rights and privileges without justifiable cause. Additionally, government agencies would have to insure the accuracy of information presented during investigations. The Mayfield case presented in the next section highlights some of the possible negative results of the government's failure to verify information in conjunction with a criminal investigation.

The Mayfield Case

The March 2004 attacks against commuter trains in Madrid, Spain, killing 191 innocent civilians, was the cause of great angst in the international community. Spanish law enforcement began their focus with an investigation of a group of Moroccans who purportedly belonged to a Morocco-based terrorist cell linked to Al-Qaeda and Osama Bin Laden, which led many to believe that the attack against the commuter trains were

either associated with the terrorist attacks on the US, or committed by Islamist extremists sympathetic to Bin Laden's cause. Investigators located a partial latent fingerprint on a bag of detonators used as part of the terror plot, and distributed them to various organizations with fingerprint databases for analysis in hopes of arresting the terrorists. One of the organizations to analyze the latent fingerprint was the FBI (Goodman 2004).

The FBI used provisions of the Patriot Act to access the fingerprints in this database, and presumably others, in hopes of finding a match. These databases produced a number of potential fingerprint matches. At least one of those potential matches existed in a database that retains the fingerprints of former US military personnel following their release from service. The fingerprint belonged to an Oregon lawyer and Muslim convert, Brandon Mayfield, who served a short stint as an officer in the US military prior to pursuing a career in law. Mayfield was unaware that his fingerprints were the focus of an investigation in the Madrid bombings. Based on the provisions of the Patriot Act, the FBI did not inform Mayfield of the investigation, nor did they ask him to sign a release granting the FBI access to his fingerprints. Upon finding the purported match, and conducting an investigation on all of the people whose fingerprints appeared to be similar to the latent fingerprint, the FBI arrested Mayfield, charged him with the terrorist act, and incarcerated him. While awaiting trial, Mayfield denied any involvement in the incident, stated that his arrest was a mistake, and claimed that the FBI arrested him based on his status as a Muslim convert (Eggen 2006).

The FBI states that his status, as a Muslim convert did not lead their investigators to arrest Mayfield; however, his religious status did play a role in the FBI's refusal to reconsider its stance when Spanish officials claimed that the latent fingerprint did not

belong to Mayfield. After a thorough investigation, Spanish officials concluded that the latent fingerprint belonged to Algerian national, Ouhnane Daoud. Following these findings, the FBI released Mayfield and apologized for the error. In November 2006, Mayfield received $2 million from the US government to pay for damages incurred as a result of his wrongful arrest (Eggen 2006).

In this case, law enforcement officials used the Patriot Act was used to supersede provisions of the Privacy Act in order to allow the FBI to conduct a search of Army databases to locate Mayfield's fingerprint. Mayfield's case gained much attention, but the media has not focused their attention on the other victims of this case, namely, all of the other former military personnel whose fingerprints exist in the same database. Under the Patriot Act, in extreme circumstances such as these, the government may search a variety of databases to aid in the capture of suspected terrorists. The ideal way to handle this problem is the use of informed consent. If the US government takes steps to inform private citizens of the potential uses of their biometrics at the time of enrollment, then government officials will meet the requirement of informed consent.

Suitability

Like COA 2, this COA would produce a database primarily populated with biometric data of US citizens. Though as stated previously, a COA of this type would be of great value to local authorities in the prosecution of local crimes; it does not incorporate the biometric information of non-US citizens. In order to increase the suitability of this COA for the intended purpose, the biometric databases created by this system would have to be interoperable with existing databases to maximize effectiveness by capturing and comparing biometric information of both US and non-US citizens.

Acceptability

Though the technology exists to create a system that collects biometrics in the manner, it is likely that many Americans would object to the intrusive nature of this collection. As stated in chapter 1, many Americans deeply value their privacy, and they would not desire to reveal personal information to the US government without adequate cause. The US government's failure to adequate protect information from compromise in the past would likely hurt any attempt to collect and store biometric information of all US citizens. Many Americans would also likely feel coerced into providing their biometric data to government officials if collection were a prerequisite to obtaining a service available to all US citizens. It would be very difficult to opt out of such a system because for many people, daily life depends on their ability to obtain and maintain driver's licenses and other credentials, which would be unavailable to them if they chose to opt out of the system.

Preferred Course of Action

Based on the analysis of each COA, it appears that the most viable COA is COA 2-mandatory biometric collection against properly detained personnel, while merging existing government criminal databases to form master data networks used by law enforcement to prosecute the GWOT. A program that requires mandatory collection of biometrics using a three-biometric format meets the legal requirements as dictated by the Fourth, Fifth, and Fourteenth Amendments. This is evident because many law enforcement agencies currently require mandatory biometric sampling of properly detained personnel. The requirement to collect the biometrics in compatible formats would allow for unprecedented interoperability and accuracy when identifying

individuals. It does not have the drawback of causing undue attention from the public as similar systems are currently in use throughout the US. The next chapter further discusses the implications of using the accepted COA and suggests further research into the application of biometrics as a part of security plans for a number of US government agencies in support of the GWOT.

CHAPTER 5

CONCLUSIONS AND RECOMMENDATIONS

The last chapter presented and analyzed three COAs to determine their feasibility, acceptability, and suitability for implementation by the US government as part of a security program directed to prosecute the GWOT. This chapter highlights the merits of COA 2 while giving due acknowledgement to the limitations inherent in the implementation of the solution. The chapter ends with a discussion of further research required to harness the power of biometrics for use by the US government.

Conclusions

As stated in chapter 3, many law enforcement agencies currently require properly detained personnel to submit to photographing as well as fingerprinting as part of a prisoner intake process. The fact that this methodology is already in use by many law enforcement agencies without significant legal pitfalls is an indication that the mandatory implementation of such a policy throughout the law enforcement domain is quite possible without significant legal hurdles. The key to maximizing the effectiveness of such a strategy would be to mandate the adoption of the program at all levels, and to ensure that the programs implemented capture, store, and retrieve the biometric templates in interoperable formats. This will allow all law enforcement entities to enroll biometric data of known or suspected terrorists and other criminals into criminal and terrorist databases. It will also allow them to query the databases using collected biometric information to determine if the biometric data collected matches templates that exist in the databases. Ideally, law enforcement official would also be able to query databases

owned by US-VISIT/IDENT, the IAFIS, and other databases to identify known or suspected criminals.

In addition to the mandatory collection of all three biometrics from properly detained persons, the US government should adopt a parallel protocol for the collection and enrollment of biometrics of all persons entering and exiting the US. As stated in chapter 3, US citizens' rights and privileges do not apply universally to foreign visitors. The US government currently collects fingerprints from all persons attempting the cross US borders as part of the US-VISIT/IDENT system (Global Security.org 2007). A searchable biometric database containing biometric information from properly detained personnel as well as personnel entering and exiting the US greatly expands the biometric library which security personnel may use to identify and capture known or suspected terrorists and other criminals.

Consider the following example to highlight the merits of such a system. According to the Center for Immigration Studies, Zacarias Moussaoui, and three of the alleged highjackers responsible for the 9/11 terrorist attacks had all overstayed their visas (Camarota 2007). If the system described above were in use at the time of terrorist attacks, the US-VISIT/IDENT systems would have flagged their biometric information, alerting all law enforcement personnel of the violation. If the police apprehended and detained the terrorists, they would have collected the terrorists' biometric information and entered it for comparison with other biometric databases to determine if the individuals had outstanding warrants. Once the crime database interacted with the US-VISIT/IDENT database, the arresting officer would have identified them as having overstayed their visas, and began processing them for deportation. In the event that they did not come in

contact with the police, security cameras in the airports would have captured their facial geometries and compared them to those in existing databases. The system would have matched their faces with those found in the US-VISIT/IDENT database, and security officials in the airport would have immediately arrested them and processed them for deportation. Admittedly, the implementation of COA 2 would not guarantee the capture of all terrorists, but this scenario demonstrates the powerful implications of such technology.

Recommendations

Using this protocol would also be of significant value to law enforcement organizations. Capturing photos of known and suspected criminals and placing them on file assists in the creation of a lineup that law enforcement officials may use as part of a criminal investigation. Most law enforcement agencies currently capture photos for one on one comparison when a witness to a crime is available to identify the individual based on physical characteristics. This allows witnesses to crimes to view photographs of potential suspects. The witness may view numerous pictures of suspects to determine whether a picture in the lineup matches the witness's mental picture of the suspect. If the witness can identify a suspect from the lineup based on his memory of the suspect, law enforcement officials may investigate the activities of the suspect to determine whether he committed the crime. In some cases, law enforcement agencies utilize forensic artists to draw pictures of the suspect as remembered by the witness. Investigators then circulate the composite picture in hope that individuals will recognize the picture and provide information to the police concerning the identity and whereabouts of the suspect. Systems such as these are useful when the identity of the perpetrator is unknown, and

there is a media through which technicians may circulate the composite picture among a large group of people (Taylor 1999). The major drawback of the use of such a system is that it relies on the right person to see the picture and to report information about the suspect. In some cases, the potential witness may not see the picture during circulation, or he may be unwilling to report his knowledge of the suspect to the police.

Biometric facial recognition would present law enforcement officials unprecedented functionality in cases such as the ones mentioned above. An automated system, appropriately designed, would allow law enforcement personnel to enter facial data, as described by a witness, into a software program that would search databases for the facial matches based on the witness's report, producing a digital lineup of possible suspects from which the witness may select. It also reduces the need for artists to draw renditions of suspects' faces as part of a criminal investigation. An appropriate program would essentially draw a rendition of the suspect based on the witness's report, reducing the amount of time required to draw artists' renditions, and reducing the overall need for the artists. Since many commercial and government businesses use security cameras, security officials may send digital photos of suspects committing crimes to a crime laboratory where investigators may compare the digital photo caught by the security cameras to those in the criminal database producing a lineup of possible suspects providing greater focus to police investigations. Such a system would require additional research in the area of facial recognition to improve the available technologies prior to implementation, but would be quite worthy of research as it would assist in the identification of terrorists and other criminals.

Technological improvement in the area of facial recognition holds great promise. As stated previously, facial recognition technologies are still in relative infancy. Suspects may fool the current systems by simply changing their facial expressions. Other variables such as lighting and resolution require the development of complex algorithms to improve the overall quality of the systems, and to reduce the ability to fool the systems. Given time, research, and development, security cameras at borders, airports, and other points of entry to the US will collect facial data from each person entering and exiting the area, and compare it to facial data in crime databases and terrorist watch lists greatly improving the US government's ability to identify and detain suspected terrorists and other criminals.

Facial recognition functionality would be quite valuable to USCG and the Border Patrol in their quest to reduce the flow of illegal immigrants into the US. Currently, the system used to capture suspected illegal immigrants in the Mona Pass, as described previously, does not have a facial recognition component. The protocol calls for the capture of a digital photo; however, this photo only allows the cutter crews and other involved in investigating suspected illegal immigrants, to verify the identity of the immigrants. The system does not collect a biometric template of facial features that allows for the query of databases containing facial recognition data to verify the identity of the detained suspect. The system relies on digital fingerprinting technology to identify the illegal immigrants. The system also lacks the ability to collect iris scans from the suspects (Amerson 2007).

Though it may seem that the collection of multiple biometrics from potential illegal immigrants may be unnecessary, based on the number of personnel attempting to

enter the US via the Mona Pass and other water routes, one must consider that many illegal immigrants may be involved in drug trafficking, human trafficking, terrorist activity, or other crimes. Additionally, one must consider the large influx of illegal immigration across US borders. The porous nature of the borders shared with Canada and Mexico make it imperative that the US take serious action to secure the borders to prevent the infiltration of terrorists and other criminals across the borders. Implementing a multi-biometric collection security program at the border would serve as a significant deterrent against those who would cross the borders illegally, as has been demonstrated in the Mona Pass.

The collection of multiple biometrics reduces the possibility of incorrectly identifying personnel, even when the suspect has attempted to alter some of his biometrics. The more biometric data available on an individual, the less likely it will be for the system to produce false matches, as the probability of the people, even identical twins, sharing multiple biometrics is very low. It is therefore quite beneficial to implement a multiple biometric collection program for use by the USCG to enhance their ability to capture and detained suspected terrorists and other criminals. As previously stated, all biometric information collected and enrolled by government officials should be stored in a format that allows for the query of the database by all law enforcement organizations. In this case, it would assist in detention of personnel who repeatedly attempt to enter the US borders illegally, as well as assist in the detention of known or suspected terrorists.

Given the proven and potential effectiveness of the use of fingerprints and digital photos, one might ask why a third biometric is necessary as part of the security plan. As

stated in chapter 3, some have made attempts, in the past to alter their fingerprints with the intent of fooling biometric devices. Though law enforcement personnel have caught a number of criminals who attempted to hide their identities in this manner, it is not possible to know how many people have been successful at fooling the systems. Both facial features and fingerprints are subject to alteration; however, it would be much more difficult to alter one's iris. As stated in chapter 1, the blood vessels of the eye remain relatively stable throughout life, and they quickly deteriorate following death. Given the risk to one's sight, it would seem quite inconceivable that one would attempt to alter blood vessels in his eyes in an attempt to evade identification. There may come a time in the future when contact lenses are developed to fool the system; however, anyone attempting to hide his identity would also have to change his facial features and fingerprints as well. The UAE demonstrated the immense effectiveness of the use of iris scans as part of their border security program. I believe that the use of multiple biometrics enhances such a plan.

COA 2 acts within the boundaries of the Fourth Amendment, as biometric collection in this fashion does not constitute an unreasonable search or seizure. Recall that case law has already demonstrated that collection of physiologically based information such as fingerprinting and drug testing constitutes reasonable searches, particularly when dealing with properly detained personnel. Additionally, the US-VISIT/IDENT System mandates biometric collection against individuals as they enter and exit US borders. The major challenge would not be the legality of the search or seizure, but the cooperation of individual states in such an initiative, and the development

of the infrastructure necessary to collect all biometric information in compatible formats, and to build secure databases for information sharing amongst law enforcement agencies.

COA 2 also adheres to the Fifth Amendment's call to collect biometrics using the least invasive procedures. All three biometrics associated with the COA are collected using unobtrusive means. The current technology allows for collection of all three biometrics without penetrating the skin, which appears to be vital in the determination of whether or not the collection technique appears to be excessively intrusive. Additionally, the US government may implement COA 2 in such a way that it does not violate the Fourteenth Amendment's right to due process. To ensure the public's right to due process, the US government would have to ensure that all biometric collection practitioners receive adequate training and certification on both the use of the biometric collection devices, and on the use of the associated databases to ensure accuracy of collection, storage, retrieval and comparison of records. The judicial system would serve to adjudicate cases where the legitimacy of biometric information and matching come into question.

In addition to protecting the constitutional rights of its citizens, the US government would have to establish a secure means to store the biometric information in keeping with the Privacy Act. The system would necessarily take advantage of encrypted computer and digital technologies. The US government would have to provide adequate safeguards to prevent the compromise of biometric information on file. As previously stated, identity theft using biometrics may not be recoverable since unlike the SSN, biometrics cannot be reissued in the event of compromise. This database would also

require protection from terrorists and other criminal who may seek to manipulate or alter the information contained in the databases.

The US government may implement COA 2 without expanded provisions of the Patriot Act or similar legislation. The US government and law enforcement personnel have the right to collect biometrics of both properly detained personnel and personnel entering and exiting the US without the use of the Patriot Act. Many criminal databases currently interact with those of the US-VISIT/IDENT system without the use of the provisions of the Patriot Act. The major difference between the current protocols and the one suggested by COA 2 is that COA 2 mandates the collection of three biometrics from this population, using compatible formats, and that all of the databases interact with each other to identify individuals. The US government may implement COA 2 with limited legal concerns with regard to the Fourth, Fifth, and Fourteenth Amendments, and the Privacy Act.

Though the implementation of COA 2 paints a rosy picture for those endeavoring to protect citizens of the US from terrorist and other criminal activity, it does present drawbacks. It is likely that once the US adopts such a robust biometric collection protocol; peer countries would implement similar programs for the protection of their own borders. This poses a significant challenge for persons that may attempt to enter foreign countries using alias names and documents. This may occur when high-ranking government officials travel using alias names for their own protection, as they are high value targets to terrorist or hostile government organizations. Not all countries practice biometric collection, and those countries that collect biometrics do not all collect them in the same format. High-ranking officials may take advantage of the inequities by using

fixed names and documents for entering and exiting different countries. Though the governments of other countries would collect their biometrics, they would link the biometric information to an alias personality, which my serve the desired purpose.

In addition to creating a challenge for US officials traveling in alias name, the protocol may provide terrorists with intelligence that they need to seek, capture, detain, or murder high value officials. COA 2, fully implemented would cause the creation of a massive database of biometric information linked to any person properly detained in the US, and all personnel entering and exiting the US. This provides terrorist organizations foreign governments, or other interested parties an opportunity to steal or alter information in the database for their own purposes. Outside personnel and organizations may seek to alter information in the database, causing the misidentification of personnel. They would also seek to delete criminal records to allow people on terrorist watch lists, and other criminals to infiltrate the US undetected. To implement this COA, the US government must take greater care in encrypting and protecting information from compromise.

Americans deeply value their rights and freedoms; however, the US government may have to infringe upon their rights and privacy to protect its citizens, critical infrastructure, and key resources from attack by terrorists and other criminals. Though COA 2 may cause some concern within the US citizenry who are very cautious about allowing the government to invade their privacy to protect their freedoms, US citizens must come to understand that security comes at a price. Ultimately, the US public must determine what price they are willing to pay in terms of their privacy, to allow the government to protect the nation from terrorist attack.

REFERENCE LIST

Adkins, Laura D. 2007. "Biometrics: Weighing convenience and national security against your privacy." 13 Mich. Telecomm. Tech. L. Rev. 541. http://www.mtlr.org/volthirteen/adkins.pdf (accessed February 12, 2008).

Amerson, Thomas. 2007. "Privacy impact assessment update: U.S. coast guard biometrics at sea program." http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_uscg_monapass_update.pdf (accessed February 15, 2008).

Anti-Defamation League. 2007. "Militia of Montana." http://www.adl.org/learn/ext_us/mom.asp?xpicked=3&item=mom (accessed December 20, 2007).

Bhagavatula, Vijayakumar. 2007. "Computer systems and security intelligent systems signal processing, multimedia and sensor exploitation systems." http://www.cylab.cmu.edu/default.aspx?id=48 (accessed March 2, 2008).

Biometric Consortium Conference. 2008. "Understanding privacy laws." http://www.biometrics.org/bc2005/Presentations/Conference/1%20Monday%20September%2019/Mon_Ballroom%20E/Fineburg%20-%20Understanding%20Privacy%20Laws.pdf (accessed February 15, 2008).

Biometrics Task Force. 2007. "Biometrics use cases." http://www.biometrics.dod.mil/ReferenceTutorials/BiometricUseCases/tabid/85/Default.aspx (accessed October 21, 2007).

Bryant, Lynn. 2007. "The face of new surveillance-incorporating biometric face recognition into a surveillance video camera system." http://www.video-serveillance–guide.com/surveillance-video-camera-system.htm (accessed March 17, 2008).

Cafeteria Workers v. McElroy, 367 U.S. 886 (1961).

Camarota, Steven A. 2002. "How the terrorists get in." *The Public Interest* (Fall 2002). http://www.cis.org/articles/2002/sacpiarticle.html (accessed December 17, 2007).

CSI Effect.com. 2007. "The myth of CSI: Is forensic science the panacea of justice?" http://www.the-csi-effect.com/index.html (accessed December 17, 2007).

Daconta, Michael, and Anthony Iasso. 2006. "Biometrics and person-centric KM." http:\\events.fcw.com/events/2006/km/downloads/KM06_3-5_Daconta.pdf (accessed March 27, 2008).

Davis v. Mississippi, 394 U.S. 721, 727 (1969).

Department of Homeland Security. 2005. "IDENT/IAFIS interoperability." http://www.dhs.gov/xlibrary/assets/foia/US-VISIT_IDENT-IAFISReport.pdf (accessed November 14, 2007).

Eggen, Dan. 2006. "U.S. settles suit filed by Ore. lawyer." *Washingtonpost.com*; November 30. http://www.washingtonpost.com/wp-dyn/content/article/2006/11/29/AR2006112901179.html (accessed November 16, 2007).

Electronic Privacy Information Center. 2007. "Face recognition." http://epic.org/privacy/facerecognition/ (accessed October 17, 2007).

———. 2008. "The social security number as a standard universal identifier." http://epic.org/privacy/hew1973report/c7.htm (accessed February 19, 2008).

Federal Bureau of Investigation. 2007. "Integrated automated fingerprint identification system or IAFIS." http://www.fbi.gov/hq/cjisd/iafis.htm (accessed December 17, 2007).

Federal Trade Commission. 2008. "About identity theft." http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html (accessed February 10, 2008).

Feder, Barnaby. 2003. "Technology; face-recognition technology improves." *New York Times*; March 14. http://query.nytimes.com/gst/fullpage.html?res=9805E0D9103EF937A25750C0A9659C8B63 (accessed March 10, 2008).

Friedlos, Dave. 2007. "Trial of airport facial recognition system deemed a success." *Computing*; April 18. http://www.computing.co.uk/computing/news/2187984/trial-facial-recognition (accessed December 12, 2007).

Gaensslen, Robert E., and Henry C. Lee. 2001. *Advances in fingerprint technology*. 2nd ed. New York: CRC Press.

Global Security.org. 2007. "IDENT-IAFIS." http://www.globalsecurity.org/security/systems/ident-iafis.htm (accessed November 13, 2007).

———. 2008. "Fingerprint identification systems." http://www.globalsecurity.org/security/systems/biometrics-fingerprint-iafis.htm (accessed February 21, 2008).

Goodman, Al. 2004. "Spain hunts 'detonator bag' man." *CNN.com*; May 28. http://edition.cnn.com/2004/WORLD/europe/05/28/spain.warrant/ (accessed November 14, 2007).

Holcomb, R. L. 1959. Review of "Fingerprints--Scotland yard and Henry Faulds," by George Wilton. *The Journal of Criminal Law, Criminology, and Police Science* 49, no. 6 (March-April): 623-624.

Kaucher, Craig. 2007. "Types of biometrics." Biometrics Task Force. http://www.biometrics.dod.mil/ReferenceTutorials/Biometrics101/TypesofBiometrics/tabid/110/Default.aspx (accessed December 15, 2007).

Kenney, Dan. 2005. "Secure transfer of electronic detainee records and biometric information using the smartcuff digital handcuff system." http://www.smartcuff.com/download/biowp.pdf (accessed October 16, 2007).

MacVicar, Sheila. 2001. "America's new war: tracing a terrorist's footsteps." *CNN.com*. http://transcripts.cnn.com/TRANSCRIPTS/0109/25/se.12.html (accessed March 1, 2008).

Mrowka, Molly J. 1996. *Criminal procedure: Identification by use of thumbprints*. Sacramento, CA: McGeorge School of Law, University of the Pacific

National Center for State Courts. 2008. "Iris scan." http://ctl.ncsc.dni.us/biomet%20web/BMIris.html (accessed March 10, 2008).

National Center for State Courts. 2008. "Retinal scan." http://ctl.ncsc.dni.us/biomet%20web/BMRetinal.html (accessed March 10, 2008).

National Treasury Employees Union v. Von Raab, 489 U.S. 656 (1989).

Onley, Dawn S. 2004. "Biometrics on the front line." *Government Computer News*. http://www.gcn.com/print/23_23/26930-1.html (accessed November 10, 2007).

Orwell, George. 1949. *1984*. London: Seeker and Warburg.

Patriot Act of 2001. Public Law 107-56, Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism.

Pentagon Channel Recon. 2008. "Perilous passage." http://www.pentagonchannel.mil/ (accessed February 17, 2008).

Perkey v. Department of Motor Vehicles (1986) 42 Cal. 3d. 185.

Rochin v. California, 342 U.S. 165 (1953).

Rosenweig, Paul, Alane Kochems, and Ari Schwatz. 2004. "Biometric technologies: Security, legal, and policy implications." *The Heritage Foundation*. http://www.heritage.org/Research/HomelandSecurity/lm12.cfm (accessed January 24, 2008).

Rutherford, Emelie. 2001. "Facial-recognition tech has people pegged." http://archives.cnn.com/2001/TECH/ptech/07/17/face.time.idg/ (accessed February 2, 2008).

Skinner v. Railway Labor Executives'Assn., 489 U.S. 602, 617 (1989).

Social Security Administration. 2007. "Identity theft and your social security number." http://www.ssa.gov/pubs/10064.html (accessed November 13, 2007).

Taylor, Karen T. 1999. *Forensic art and illustration*. Washington, DC: CRC Press.

Tactical Biometrics on the Battlefield. "Last tactical mile vs First tactical mile, 2007." Michigan v. Sitz, 496 U.S. 444 (1990).

Transportation Security Administration. 2008. "Tips for the screening process." http://www.tsa.gov/travelers/airtravel/specialneeds/editorial_1567.shtm (accessed January 13, 2008).

Willing, Richard. 2004a. "Identical twins complicate use of DNA testing." *USA Today*. http://www.usatoday.com/news/nation/2004-06-03-twins-dna_x.htm (accessed October 15, 2007).

———. 2004b. "Twin suspects spark unique DNA test." *USA Today*. http://www.usatoday.com/tech/science/genetics/2004-09-01-dna-twins_x.htm (accessed October 15, 2007).

Wilson, C. L. 2004. "NIST patriot act biometrictesting." Conference presentation. http://www.biometrics.org/bc2004/Presentations/Conference/2%20Tuesday%20September%2021/Tue_Ballroom%20B/2%20NIST%20Session/1%20Wilson_Presentation.pdf (accessed December 13, 2007).

Woodard, John D. Jr. 2005. "Using biometrics to achieve identity dominance in the global war on terrorism." *Military Review* (September-October).

Woodward, John D. Jr., Christopher Horn, Julius Gatune, and Aryn Thomas. 2003. *Biometrics: A look at facial recognition*. Santa Monica, CA: RAND Corporation.

Woodward, John D., Karl Ware, Jr., Christopher M. Mills, Nicholas M. Orlans, John D. Woodward, Jr., and Peter T Higgins. 2002. *Biometrics*. New York: McGraw-Hill.

Woodard, John D. Jr., Katharine W. Webb, Elaine M. Newton, Melissa Bradley, and David Rubenson. 2001. *Army biometrics aApplications: Identifying and addressing sociocultural concerns*. Santa Monica, CA: RAND Corporation.

USA.gov. 2007. "Latest information on veterans affairs data security." http://www.usa.gov/veteransinfo.shtml (accessed December 14, 2007).

INITIAL DISTRIBUTION LIST

Combined Arms Research Library
U.S. Army Command and General Staff College
250 Gibbon Ave.
Fort Leavenworth, KS 66027-2314

Defense Technical Information Center/OCA
825 John J. Kingman Rd., Suite 944
Fort Belvoir, VA 22060-6218

Mr. O. Shawn Cupp
DLRO
USACGSC
100 Stimson Ave.
Fort Leavenworth, KS 66027-2301

BG William D. R. Waff
P.O. Box 1246
Coraopolis, PA 15108-6246

LTC Misti Stowell
USACGSC
100 Stimson Ave.
Fort Leavenworth, KS 66027-2301